Elektroniske spor fra mobiltelefoner

- om politiets bruk og teleoperatørenes lagring av trafikkdata

Kandidatnr: 272
Veileder: Lena Lundgreen
Leveringsfrist: 03.05.2004

Til sammen 17 993 ord

Dato: 30.04.04

Innholdsfortegnelse

1 INNLEDNING 1

1.1 BAKGRUNN, TEMA OG PROBLEMSTILLING 1

1.2 TERMINOLOGI 3

1.2.1 TRAFIKKDATA 3

1.3 RETTSKILDER, KILDER OG METODEBRUK 5

2 HJEMMELSGRUNNLAG FOR LAGRING AV TRAFIKKDATA 8

2.1 INNLEDNING 8

2.1.1 PERSONOPPLYSNINGSLOVEN – KONSESJON OG VILKÅR 10

2.1.1.1 Konsesjonens innholdsmessige begrensninger 12

2.1.1.2 Konsesjonens tidsmessige begrensninger 13

2.1.2 EKOMLOVEN § 2-7 - KOMMUNIKASJONSVERN M.V. 14

2.1.3 EKOMLOVEN § 2-8 - TILRETTELEGGING FOR LOVBESTEMT TILGANG TIL INFORMASJON 16

3 TELEOPERATØRENES LAGRINGSPRAKSIS 18

3.1 TELENOR 18

3.2 NETCOM 19

3.3 ER TELEOPERATØRENES LAGRINGSPRAKSIS LOVLIG? 20

3.3.1 TELENORS PRAKSIS FOR SLETTING AV DATA 20

3.3.2 NETCOMS PRAKSIS FOR SLETTING AV DATA 21

3.3.3 INNHOLDET I TELEOPERATØRENES LAGRINGSPRAKSIS 22

3.4 BURDE VI HA PLIKT TIL Å LAGRE TRAFIKKDATA? 24

4 BRUK AV TRAFIKKDATA I PRAKSIS 27

4.1 INNLEDNING 27

4.2 HISTORISKE SAMLEDATA 29

4.3 HISTORISKE POSISJONSDATA 29

4.4 FREMTIDIGE TRAFIKKDATA 30
4.5 TRAFIKKDATA I SANNTID 31

5 HJEMMELSGRUNNLAG FOR BRUK AV TRAFIKKDATA 33

5.1 INNLEDNING 33
5.1.1 EKOMLOVEN § 2-9 - TAUSHETSPLIKT 34
5.2 UTLEVERING AV TRAFIKKDATA UTEN BRUK AV TVANGSMIDLER 34
5.2.1 FRIVILLIG UTLEVERING ETTER FRITAK FRA TAUSHETSPLIKTEN 35
5.2.2 VITNEFORKLARING SOM FØLGE AV RETTENS KJENNELSE 38
5.2.3 FELLES OM FORKLARING ELLER UTLEVERING ETTER STRPL. § 118 38
5.2.4 SAMTYKKE FRA ABONNENT 40
5.2.5 NØDRETT 43
5.3 UTLEVERING AV TRAFIKKDATA SOM STRAFFEPROSESSUELT TVANGSMIDDEL 47
5.3.1 FORHOLDSMESSIGHETSPRINSIPPET 48
5.3.2 UTLEVERING ETTER REGLENE OM BESLAG OG UTLEVERINGSPÅLEGG 49
5.3.3 UTLEVERING ETTER REGLENE OM KOMMUNIKASJONSKONTROLL 51

6 AVSLUTTENDE BEMERKNINGER 54

7 LITTERATURLISTE/KILDER 56

VEDLEGG:

KONSESJON TIL BEHANDLING AV PERSONOPPLYSNINGER – BEHANDLING AV OPPLYSNINGER OM ABONNENTERS BRUK AV TELETJENESTER

1 Innledning

1.1 Bakgrunn, tema og problemstilling

I kjølvannet av den teknologiske utviklingen følger også en utvilkling på de fleste andre livsområder. Jus er intet unntak, men i forhold til teknologien er utvikling av lover og regler en langt mer tidkrevende prosess. Konsekvensen av dette er at den lovgivning som skal regulere bruken av moderne teknologi i mange tilfeller er utdatert allerede når den trer i kraft.

Et område hvor teknologien har utviklet seg særlig de siste årene er kommunikasjon. På syv-åtte år har mobiltelefoner og internett gått fra å være kuriositeter, til hjelpemidler de fleste er mer eller mindre avhengige av i det daglige. Norge ligger helt i verdenstoppen når det gjelder både antall mobiltelefoner[1], og tilgang på internett[2].

Et annet område hvor det i Norge er sterk vekst er antallet registrerte lovbrudd[3], og det er en sammenheng mellom økt bruk av tekniske hjelpemidler og økt kriminalitet. Det er riktignok ingen grunn til å tro at den teknologiske utviklingen i særlig grad bidrar til å øke kriminaliteten, men statistikken viser oss at den befolkningsgruppen med størst tilgang til mobiltelefoner og internett står for den største delen av de kriminelle handlinger.[4] Moderne kommunikasjonsformer, og spesielt bruk av mobiltelefon, har blitt et av de viktigste hjelpemidler i kriminell virksomhet. Dette gjelder i særlig grad alvorlig kriminalitet som narkotikaomsetning og andre organiserte forbrytelser.

---

[1] 83,2 pr. 100 innbyggere , Statistisk årbok 2003, tabell 519

[2] 68 % av befolkningen , Bruk av IKT i Husholdningene, SSB 2003, tabell 1

[3] Norsk Kriminalstatistikk 2002, tabell 4 Lovbrudd anmeldt, etter type lovbrudd. 1991-2002

[4] Bruk av IKT i Husholdningene, SSB 2003, tabell 1, og Norsk Kriminalstatistikk 2000 tabell 14.

I tråd med den teknologiske utviklingen får også politiet nye metoder og muligheter for etterforskningen av de kriminelle handlinger. Dagens teknologi har på mange områder gitt politiet en ny hverdag, med muligheter man ikke engang kunne drømme om for bare ti år siden. Med unntak av meget avansert kryptert overføring kan i praksis all kommunikasjon ved bruk av mobiltelefoner og datamaskiner på en eller flere måter overvåkes eller kontrolleres.

Temaet for denne oppgaven er teleoperatørenes lagring og politiets bruk av trafikkdata, nærmere bestemt den informasjon som produseres i forbindelse med bruk av mobiltelefoner. Av hensyn til oppgavens omfang har jeg funnet det hensiktsmessig å avgrense mot trafikkdata fra bruk av PC og andre kommunikasjonsmidler. Hjemmelsgrunnlagene for utlevering av trafikkdata er i hovedsak de samme uavhengig av hva slags kommunikasjonsmiddel som har vært brukt, og det er for øvrig lite som skiller problemstillinger rundt bruk og lagring av de forskjellige typer data fra hverandre. Jeg finner derfor en slik avgrensning fornuftig, fordi en behandling av flere former ville ha medført mye ekstra teknisk redegjørelse og lite selvstendig juridisk materiale. Bruk av trafikkdata fra mobiltelefoner er dessuten langt mer utbredt enn bruk av trafikkdata fra alle andre kommunikasjonsmidler til sammen. Når jeg i det følgende snakker om trafikkdata mener jeg trafikkdata fra bruk av mobiltelefoner. Videre vil jeg avgrense mot den bruk av trafikkdata som foregår i regi av Politiets Sikkerhetstjeneste (PST), og de spesialregler som gjelder ved brudd på Almindelig borgerlig Straffelov 22. mai 1902 nr. 10 (straffeloven) kapittel 8 [5] og kapittel 9 [6].

Bruk av ekstraordinære etterforskningsmetoder er sterkt knyttet til sentrale menneskerettigheter. Av hensyn til oppgavens omfang har jeg dessverre måttet avgrense mot en nærmere behandling av hvordan de internrettslige reglene forholder seg til Norges folkerettslige forpliktelser.

All bruk og lagring av trafikkdata oppfordrer til en debatt om hvor langt vi er villige til, og kan tillate oss, å gå for å beskytte samfunnet mot kriminalitet. Målsetningen er å

[5] Forbrytelser mod Statens Selvstændighed og Sikkerhed

[6] Forbrydelser mod Norges Statsforfatning og Statsoverhoved

begrense den alvorlige kriminaliteten[7] uten å tråkke over grensene for betryggende rettssikkerhet og personvern. Jeg skal i denne oppgaven redegjøre for, og vurdere, den internrettslige lovgivning og praksis på områdene lagring og bruk av trafikkdata som ledd i bekjempelsen av kriminalitet.

1.2 Terminologi

Oppgaven inneholder en del ord og uttrykk av teknisk karakter, spesielt i forbindelse med redegjørelsene for teleoperatørenes lagringspraksis og politiets og påtalemyndighetens bruk av trafikkdata. Disse ordene har som regel ingen juridisk betydning, og er derfor definert eller forklart fortløpende i teksten.

1.2.1 Trafikkdata

Det nærmeste som kan kalles en legaldefinisjon av trafikkdata finnes i ekomforskriften § 7-1 første ledd siste setning. Trafikkdata er her definert som ”data som er nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring”. Ordlyden i definisjonen er gitt uavhengig av hvilket kommunikasjonsmiddel trafikkdataene stammer fra, og beskriver ikke spesifikt trafikkdata fra mobiltelefoner. Definisjonen inneholder likevel ingen elementer som kan sies å være uriktig for trafikkdata fra mobiltelefoner, og kan derfor godt leses som en definisjone av den type trafikkdata jeg skal behandle i denne oppgaven. Beskrivelsen i ekomforskriften er ordrett hentet fra Ot.prp. nr. 58 (2002-2003) om lov om elektronisk kommunikasjon (ekomloven), side 92. Begrepet er der videre presisert på følgende måte: ”Med trafikkdata menes f.eks. data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet og underliggende tjeneste”.

Trafikkdata fra bruk av mobiltelefoner omfatter med andre ord all informasjon som oppstår i tilknytning til bruken, og som er nødvendig for å overføre kommunikasjonen i nettet eller faktureringen av slik overføring. Begrepet kan på grunnlag av ordlyden i ekomforskriften avgrenses mot to beslektede typer data. Det fremgår av definisjonen at data som *ikke* er nødvendig for overføring av kommunikasjon eller fakturering, ikke er å anse som trafikkdata. Dette avgrenser for det første mot informasjon som er uavhengig

[7] Ot.prp. nr. 64 (1998-99) Om lov om endringer i straffeprosessloven og straffeloven mv.

av konkret bruk (trafikk). Denne type data kalles abonnementsopplysninger, og inkluderer for eksempel hvem som er registrert som eier eller bruker av et bestemt abonnement eller apparat, jf. unntaket i ekomloven § 2-9 tredje ledd. For det andre avgrenser ordlyden i ekomforskriften trafikkdata mot innholdsdata, altså det som blir sagt i en samtale eller sendt i en melding. Kontroll med slike data er regulert i straffeprosessloven § 216a.

De data som etter dette utgjør trafikkdata kan deles inn i samledata og posisjonsdata[8]. Samledata er teleoperatørenes registreringer av alle samtaler mellom mobiltelefoner, som blant annet inneholder opplysninger om samtalens varighet samt identifisering av avsender og mottaker. Posisjonsdata gir informasjon om hvor en mobiltelefon befinner seg, eller har befunnet seg, til et bestemt tidspunkt. I forbindelse med politiets bruk av trafikkdata deles dataene videre inn som historiske eller fremtidige, avhengig av når de oppsto i forhold til tillatelsen til kontroll. Et særlig tilfelle er dessuten sporing ved hjelp av trafikkdata i sanntid. Politiets bruk av trafikkdata i de forskjellige tilfeller er nærmere redegjort for i kapittel 4.

Trafikkdata fra samtaler registreres med både telefonnummeret som blir brukt og håndsettets spesifikke identifikasjonsnummer. Hvem som står bak en samtale kan følgelig identifiseres på to måter.

Telefonnummeret identifiseres ved hjelp av IMSI-nummeret. IMSI (International Mobile Subscriber Identity) er et unikt 24-sifret nummer knyttet til hvert enkelt mobilabonnement. IMSI-nummeret er registrert og lagret i SIM-kortet (Subskriber Identity Module), og kan i prinsippet flyttes fra håndsett til håndsett.

(etterforskningsmetoder m v) s. 7

[8] Ekomforskriften bruker i § 7-2 begrepet lokaliseringsdata. Lokaliseringsdata angir den geografiske plasseringen av en mobiltelefon eller tilsvarende, men er per definisjon andre data enn de trafikkdata som faller inn under betegnelsen posisjonsdata. Forskjellen er at lokaliseringsdata ikke er nødvendige for fakturering eller oppkobling av tjenesten. Lokaliseringsdata tilbys i forbindelse med spesifikke tjenester, f.eks. peiling av stjålne fritidsbåter og biler hvor det på forhånd er utplassert en GSM-sender og et SIM-kort.

Ethvert håndsett er på sin side utstyrt med sitt spesifikke 15-sifrede IMEI-nummer. IMEI står for International Mobile Equipment Identifier og overføres automatisk av telefonen når nettverket ber om det. IMEI gjør det mulig å spore (og for eksempel sperre) én enkelt mobiltelefon, uavhengig av hvilket nettverk den brukes i eller hvilket SIM-kort som brukes i apparatet.

Ved å holde kontroll med hvilke SIM-kort som brukes i kombinasjon med hvilke IMEI-numre danner politiet seg en god oversikt over de håndsett og telefonnumre som kan knyttes til en enkelt person. I denne forbindelse kan politiet, ved hjelp av metoder som kalles SIM- eller IMEI-søk, få opplysninger fra teleoperatørene om hvilke SIM- og IMEI-numre som tidligere har vært brukt sammen. Slike data er ikke ansett som trafikkdata og utleveres derfor til politiet på begjæring, jf. ekomloven § 2-9 tredje ledd og pkt. 5.1.1.

1.3 Rettskilder, kilder og metodebruk

Lagring og bruk av trafikkdata fra mobiltelefoner er et forholdsvis nytt rettsområde. Rettskildesituasjonen bærer preg av å være sammensatt av forskjellige lovverk, hvert med sine generelle regler som i større eller mindre grad også får anvendelse her. Spesifikk regulering av behandling av trafikkdata er en sjeldenhet, og jeg har av denne grunn hatt få teoretiske kilder hvor de problemstillinger jeg tar opp er drøftet konkret. Det er derfor fare for at mine vurderinger kan ha blitt unyanserte eller mangelfulle på enkelte områder.

Det er også lite tilgjengelig rettspraksis i forhold til lagring og bruk av trafikkdata. Det finnes noen Høyesterettsavgjørelser som bidrar til å trekke opp grensene for relevante strafferettslige og prosessuelle bestemmelser, men utover dette er det svært begrenset. Hovedgrunnen til dette er at de fleste rettsavgjørelser på området er kjennelser for kontroll av trafikkdata eller utsatt underretning, som fattes av den lokale tingrett. Slike avgjørelser blir normalt ikke publisert.

Teleoperatørenes lagring og behandling av trafikkdata er behandlet i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven). Denne loven er relativt ny, og er en

delvis videreføring av den opphevede lov 23. juni 1995 nr. 39 om telekommunikasjon (teleloven). Juridisk teori og rettsavgjørelser om den gamle teleloven vil ha en viss rettskildemessig vekt for tolkningen av ekomloven på de områder hvor den gamle lovteksten er videreført, eller hvor det ikke har vært meningen å gjøre realitetsendringer. I tillegg til loven gjelder forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften), som ble vedtatt av Samferdselsdepartementet den 16.02.04.

Trafikkdata er dessuten etter lov om behandling av personopplysninger (personopplysningsloven) 14. april 2000 nr. 31 er trafikkdata å anse som personopplysninger. Personopplysningsloven, forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften) og vilkårene gitt av Datatilsynet i Konsesjon til å behandle personopplysninger – behandling av opplysninger om abonnenters bruk av teletjenester for behandling av trafikkdata[9] (heretter kalt konsesjonen) utgjør derfor viktige rettskilder.

Utlevering av trafikkdata kan skje på grunnlag av et straffeprosessuelt tvangsmiddel, herunder en form for kommunikasjonskontroll. Disse er hjemlet i lov 22.mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) kapittel 16 og 16a. Forskrift om kommunikasjonskontroll, fastsatt ved kongelig resolusjon 31. mai 1995 nr. 281 (kommunikasjonskontrollforskriften) med hjemmel i straffeprosessloven § 216k, gjelder for all bruk av kommunikasjonskontroll.

Lagring og bruk av trafikkdata er i den senere tid behandlet i to offentlige utredninger. Først ute var Datakrimutvalget i NOU 2003:27 Lovtiltak mot datakriminalitet, som inneholder forslag til nødvendige lovtiltak for gjennomføring av Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi i norsk rett. Den 29. mars 2004 ble dessuten Politimetodeutvalgets NOU 2004:6 Om politimetoder i forebyggende øyemed offentliggjort, med drøftelser om bl.a. plikt til lagring og forebyggende bruk av

[9] Vedlegg 1.

trafikkdata. Sammen med tre Odelstingsproposisjoner utgjør disse NOUer viktige rettskilder for denne oppgaven, se litteraturlisten i kapittel 7 for fullstendig oversikt.

Fordelen ved manglende teoretisk og rettskildemessig grunnlag er at jeg i stor grad har måttet henvende meg til aktørene som anvender de aktuelle rettsreglene i praksis. Dette har hjulpet meg til å identifisere konkrete problemstillinger, og gitt meg forskjellige perspektiver på materialet.

2 Hjemmelsgrunnlag for lagring av trafikkdata

2.1 Innledning

Lagring av trafikkdata foregår utelukkende hos teleoperatørene, og er begrunnet i deres behov for slik informasjon i forbindelse med fakturering av kundene. På grunn av opplysningenes innhold, og fordi de blir lagret elektronisk og dermed er lett tilgjengelige og søkbare, oppsto det fort et ønske fra politi og påtalemyndighet om å få innsyn i dem. Denne bruken av overskuddsinformasjon fra teleoperatørenes lovlige lagring har utviklet seg kraftig de siste årene, i takt med den teknoligiske utviklingen, og det er ingen grunn til å tro at den vil stanse.

I Norge er det i dag tre teleoperatører som har sitt eget mobilnett: Telenor Mobil, Netcom og Teletopia. Den siste er foreløpig av helt ubetydelig størrelse både i utstrekning og antall abonnenter, og i praksis går all mobiltelefontrafikk gjennom Telenors eller Netcoms nett. De øvrige selskapene som tilbyr teletjenester, for eksempel Chess, Sense, og Tele 2, leier nettjenester fra et eller begge disse selskapene. Trafikkdata som oppstår som følge av kommunikasjon fra for eksempel Sense sine kunder blir overført fra nettleverandør til Sense, og kan i utgangspunktet begjæres utlevert derfra. Men nettleverandøren lagrer også disse trafikkdataene hos seg, som grunnlag for sin fakturering av underleverandøren (samtrafikkavregning). Ved begjæring om utlevering behøver politiet følgelig kun å henvende seg til nettleverandørene, og i praksis er det derfor bare Netcom og Telenor som utleverer trafikkdata til politi og påtalemyndighet.

Sommeren 2003, i tiden før og etter vedtagelsen av den nye ekomloven[10], pågikk det en debatt om bl.a. innføring av lovpålagt plikt til lagring av trafikkdata og forbud mot anonyme forhåndsbetalte mobiltelefonabonnementer (kontantkort). Datatilsynet og andre personvernsorganisasjoner mente at den enkeltes rett til privatliv og til å kunne

[10] Ekomloven ble vedtatt den 04.07.2003.

kommunisere anonymt, tilsa at verken lagringsplikt utover det som er nødvendig for teleoperatørene eller registrering av kontantkortabonnenter burde være lovpålagt. Aktører fra påtalemyndigheten reagerte på at ekomloven ikke inneholdt noen lagringsplikt for trafikkdata, slik som det nå er innført i bl.a. Frankrike, Belgia, Spania, Storbritannia og Danmark. De pekte på at Norge var i utakt med den gjeldende rettsoppfatningen i Europa, og mente manglende lagringsplikt og registrering av kontantkortabonnenter ville medføre at en rekke alvorlige kriminelle handlinger ikke ble oppklart. Videre ble det hevdet at lagring av trafikkdata er et så alvorlig inngrep at dette burde vært behandlet i selve lovteksten, forskriftshjemmel i medhold av lov eller retningslinjer i forarbeidene ble ikke ansett tilfredsstillende.

Lovgiver lot seg i første omgang ikke påvirke av argumentasjonen fra representantene for påtalemyndigheten, og det finnes pr. i dag ingen lovbestemt plikt til å lagre trafikkdata. Utenom til fakturerings- og kommunikasjonsformål har heller ikke teleoperatørene noen interesse i å lagre trafikkdata om sine kunder. Om vi burde ha en lovbestemt plikt til å lagre trafikkdata er et spørsmål jeg kommer tilbake til i pkt. 3.4. Ekomloven § 2-8 pålegger riktignok teleoperatørene å tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres, men innholdet i denne plikten har ikke blitt prøvet. Det syntes imidlertid klart at noen lagringsplikt ikke kan tolkes inn i denne regelen (se nærmere om ekomloven § 2-8 i pkt. 2.1.3).

I spørsmålet om registrering av kontantkortkunder har påtalemyndighetens synspunkter etterhvert fått gjennomslag. Plikt til registrering av slike kunder ble formelt pålagt ved vedtakelsen av ekomforskriften den 18.02.2004, jf. ekomforskriften § 6-2 1. ledd, jf. ekomloven § 2-8 første og tredje ledd. Netcom har frem til dette ikke registrert andre kontankorttkunder enn de som selv frivillig registrerte seg, og har i dag rundt 250 000 kunder som overhodet ikke er registrert. Telenor har alltid stilt krav om at kontankorttkunder skal registrere seg, men fordi informasjonen ikke har fungert som faktureringsinformasjon ble de oppgitte opplysninger aldri kontrollert mot folkeregisteret. Fordi slike opplysninger ikke er trafikkdata, jf. pkt. 1.3.3, faller en nærmere redegjørelse for spørsmålet om registrering av kontantkortkunder utenfor rammene av denne oppgave.

Trafikkdata er ansett som personopplysninger ihht. personopplysningsloven, jf. pkt. 2.1.1, og det gjelder derfor strenge vilkår for behandlingen (herunder lagring) av slike opplysninger. Fordi innholdet i trafikkdata er av særlig inngripende karakter, og på grunn av det meget betydelige omfanget, er det dessuten bestemt konsesjonsplikt for teleoperatørenes behandling av trafikkdata.

Ved siden av de grunnlag for lagring, eller rettere sagt de unntak fra plikten til å slette, som følger direkte av konsesjonen, åpner denne for lagring i medhold av annen lov. Slike regler finnes i ekomloven kapittel 2. Jeg skal i det følgende gjøre rede for gjeldende rett etter personopplysningsloven og ekomloven.

2.1.1 Personopplysningsloven – konsesjon og vilkår

Personopplysningsloven § 2 nr. 1 definerer personopplysninger som opplysninger og vurderinger som kan knyttes til en enkelt person. Dette inkluderer alle trafikkdata som ikke er anonymisert, eller på annen måte behandlet slik at de ikke kan knyttes til et spesifikt SIM-kort eller IMEI-nummer (og derved til en bruker). Behandling av personopplysninger omfatter etter samme paragraf nr. 2 enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter. Teleoperatørenes lagring og utlevering, samt den kontroll av trafikkdata som skjer i regi av politi og påtalemyndighet, er etter dette å betrakte som behandling av personopplysninger.

Personopplysningsloven § 11 oppstiller kumulative grunnkrav for behandling av personopplysninger. Av disse fremgår at personopplysninger bare kan behandles når dette er tillatt ihht. § 8. Etter § 8 første ledd er det en forutsetning for behandling at den registrerte har samtykket, at behandlingen er fastsatt i lov eller at et av de alternative vilkårene i bokstav a-f er oppfylt. Det finnes pr. i dag ingen lovbestemt plikt til å lagre trafikkdata, jf. pkt. 2.1, og grunnlaget for å lagre trafikkdata må derfor enten ligge i et samtykke fra abonnenten, eller etter bokstav a følge av at lagring er nødvendig for at teleoperatøren skal kunne oppfylle sin avtale med abonnenten om levering av teletjenester.

Dersom samtykke skal kunne sies å foreligge må dette etter personopplysningsloven § 2 nr. 7 være en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv. For kunder som signerer en abonnementsavtale kan dette vilkåret, avhengig av hva som står i avtaleteksten, kanskje i noen tilfeller sies å være oppfylt. Hovedregelen er nok likevel at kravet til samtykke ikke er oppfylt. Dette er helt klart for kontantkortabonnenter, som ofte verken signerer noen avtale eller får noen slik utlevert når de kjøper abonnementet sitt, men det gjelder antakelig også de fleste abonnentskunder som faktureres i ettertid. Grunnlaget for behandling (lagring) av trafikkdata er derfor i de aller fleste tilfeller personopplysningsloven § 8 bokstav a, fordi dette er nødvendig for at teleoperatørene skal kunne oppfylle sin avtale med abonnenten. Lagring av trafikkdata er nødvendig for registrering av kundens bruk av abonnementet, og dermed teleoperatørens fakturering eller debitering av ringesaldo.

På grunn av de strenge personvernshensyn som gjør seg gjeldende ved behandling av sensitive personopplysninger krever slik behandling etter personopplysningsloven § 33 første ledd konsesjon fra Datatilsynet. Trafikkdata er ikke ansett som sensitive personopplysninger etter personopplysningsloven § 9, men konsesjonsplikt kan likevel pålegges av Datatilsynet etter § 33 annet ledd ”dersom behandlingen ellers åpenbart vil krenke tungtveiende personverninteresser. I vurderingen av om konsesjon er nødvendig, skal Datatilsynet bl.a. ta hensyn til personopplysningenes art, mengde og formålet med behandlingen.” Også Kongen kan i medhold av personopplysningsloven § 31, 4. ledd gi forskrift om at visse behandlingsmåter eller behandlingsansvarlige er underlagt konsesjonsplikt. Dette er gjort i personopplysningsforskriften § 7-1, hvor tilbydere av teletjenesters behandling av personopplysninger for kundeadministrasjon, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av telenett er gjort konsesjonspliktig etter personopplysningsloven.

Personopplysningsloven §§ 34 og 35 gir videre Datatilsynet anledning til å sette rammer for behandlingen av personopplysninger, gjennom vilkår knyttet til den enkelte konsesjon. Konsesjonsplikten og konsesjonsvilkårene gjelder kun trafikkdata som knytter seg til fysiske personer, jf. personopplysningsloven § 2 nr. 1. Trafikkdata som

ikke knytter seg til fysiske personer kan derfor fritt lagres ihht. øvrig lovgivning, for i forbindelse med lagring av anonymiserte data til statistikkformål.

I konsesjonen har Datatilsynet satt en rekke vilkår for behandling av opplysninger om abonnenters bruk av teletjenester. Disse vilkårene er standardvilkår for teleoperatører, og likelydende konsesjoner er gitt til alle aktører på markedet. Konsesjoner om behandling av personopplysninger er ikke tidsbegrensede, og gjelder inntil Datatilsynet opphever eller endrer dem.

2.1.1.1 Konsesjonens innholdsmessige begrensninger

Hovedregelen i konsesjonsvilkårenes pkt. 8, ”Sletting av opplysninger”, er at opplysninger som ikke har betydning for formålet skal slettes eller anonymiseres. Formålet er etter vilkårenes pkt. 1 ”kundeadministrasjon, opplysningstjeneste, fakturering og gjennomføring av tjenester i forbindelse med abonnenters bruk av telenett, inklusive samtrafikkavregning”. Videre følger det av konsesjonens pkt. 2 at det bare kan behandles opplysninger som er nødvendige for gjennomføring og fakturering av tjenesten.

Fordi trafikkdata er bruksavhengig, og ikke sier noe om kunden som sådan (personalia, telefonnummer, abonnementstype eller lignende), er dette en type opplysninger det ikke er aktuelt å bruke i kundeadministrasjon eller opplysningstjeneste. Følgelig kan trafikkdata kun lagres i den utstrekning de har betydning for ”fakturering og gjennomføring av tjenester i forbindelse med abonnenters bruk av telenett, inklusive samtrafikkavregning”. Trafikkdata har betydning for gjennomføring av tjenester i forbindelse med bruk av telenettet, men anledningen til å lagre andre data enn de som også har betydning for fakturering på dette grunnlag opphører samtidig med at bruken er avsluttet, jf. konsesjonens pkt. 8, ”Slettefrist”, annet avsnitt.

Etter dette er trafikkdata en type opplysninger som i medhold av konsesjonen kun kan lagres i den utstrekning de har betydning for teleoperatørenes fakturering av sine kunder, eller samtrafikkavregning (som er den fakturering som skjer mellom selskapene som eier og leier telenettene).

All utgående trafikk faller etter dette inn under konsesjonen. Når det gjelder inngående trafikk er det ikke like enkelt. Utgangspunktet er naturligvis at en teleoperatør ikke kan fakturere kunden for inngående trafikk, slik at trafikkdata fra for eksempel mottatte samtaler ikke kan lagres. Det er likevel et par viktige unntak fra dette. For det første fakturerer teleoperatørene kunder som mottar samtaler i utlandet. Den som for eksempel ringer opp sin kamerat i Spania betaler selv for samtalekostnadene til riksgrensen, men det er mottakeren som må betale for merkostnadene ved bruk av utenlandske telenett. For det andre medfører ordningen med utleie av telenett at inngående trafikk fra en kunde som bruker samme nettleverandør som avsender, samtidig utgjør utgående trafikk og fakturainformasjon som nettleverandøren lagrer på denne kunden. Hvilke data som etter omstendighetene kan utleveres til politi og påtalemyndighet varierer etter hvilken bestemmelse utleveringen er hjemlet i, jf. kapittel 5.

2.1.1.2 Konsesjonens tidsmessige begrensninger

Opplysninger som brukes til faktureringsformål skal etter hovedregelen i konsesjonens pkt. 8 slettes når faktura er gjort opp, eventuelt når en klagefrist er gått ut. Videre følger det av pkt. 8 at opplysningene skal slettes senest fem måneder etter at de ble registrert ved kvartalsvis fakturering, og tre måneder etter at de ble registrert dersom kunden faktureres månedlig.

Siden hovedregelen er at dataene skal slettes når faktura er gjort opp, eller senest når klagefrist har gått ut, må maksimumsgrensene på tre og fem måneder forstås som utløp av maksimale klagefrister. Fordi fakturering skjer etterskuddsvis innebærer dette at de siste data fra en kunde som er registrert i en periode på enten en eller tre måneder, må slettes senest 60 dager etter at de er registrert. Konsesjonsvilkårene innebærer følgelig en maksimal klagefrist på 60 dager.

Unntak fra disse maksimumsgrensene gjelder dersom faktura ikke er betalt, eller det er oppstått rettslig tvist om betalingsplikten. I slike tilfeller kan opplysningene oppbevares inntil kravet er gjort opp eller rettslig avgjort. Etter at faktura er gjort opp kan det for fakturaperioden lagres navn og adresse på kunden, i tillegg til beløpet.

Opplysninger som kun er nødvendige for oppkobling eller gjennomføring av tjenesten skal slettes straks tjenesten er nedkoblet.

I siste avsnitt under overskriften ”Slettefrist” i vilkårenes pkt. 8 begrenses plikten til å slette til å kun gjelde så lenge opplysningene ikke skal oppbevares i henhold til annen lov. Det er åpnet for å gi slik lagringsplikt i ekomloven § 2-8, tredje ledd, jf. pkt. 2.1.3.

Det fremstår som en svakhet ved konsesjonen at denne ikke spesifikt tar opp problemstillingen med lagring av trafikkdata fra forhåndsbetalte abonnementer. Konsesjonens ordlyd omhandler bare kunder som faktureres månedlig eller kvartalsvis, og utelater dermed en betydelig andel abonnenter med forskjellige forhåndsbetalte abonnementer. Fordi dette er en spesiell situasjon, og ikke minst fordi den er av særlig betydning for politi og påtalemyndighet i og med at slike abonnementer er spesielt populære blant mennesker som ønsker å unndra seg kontroll, kunne det være ønskelig at Datatilsynet presiserer plikten til å slette disse dataene i konsesjonens pkt. 8. I lys av teleoperatørenes meget forskjellige praksis er det grunn til å tro at det hersker betydelig tvil om hvordan konsesjonen skal tolkes, jf. pkt. 3.1 og 3.2 flg.

Datatilsynet er i ferd med å oppdatere konsesjonsvilkårene slik at disse språklig stemmer overens med ekomloven. Det er ikke planlagt at oppdateringen vil føre til innholdsmessige endringer.

2.1.2 Ekomloven § 2-7 - Kommunikasjonsvern m.v.

Ekomloven § 2-7 inneholder regler om kommunikasjonsvern, herunder vern mot at uvedkommende får adgang til andres kommunikasjon eller data om denne. Første ledd pålegger den enkelte tilbyder å gjennomføre nødvendige sikkerhetstiltak til vern av kommunikasjon som foregår gjennom deres nett, og informasjonsplikt til abonnent dersom det oppstår særlig risiko for brudd på sikkerheten. Nødvendige sikkerhetstiltak innebærer at tilbyder plikter å oppdatere sine sikkerhetsrutiner i takt med den teknologiske utvikling, slik at sikkerheten til enhver tid fremstår som tilfredsstillende. Sikkerhetstiltakene inkluderer både tiltak for å hindre avlytting og datainnbrudd.

Annet ledd inneholder ytterligere sikkerhetstiltak for å verne trafikkdata. Hovedregelen om lagring av trafikkdata er at disse skal slettes eller anonymiseres så snart de ikke lenger er nødvendige for kommunikasjons eller faktureringsformål, med mindre noe annet er bestemt i eller i medhold av lov. Loven skiller her mellom trafikkdata som kun er nødvendig for kommunikasjonsformål, og trafikkdata som i tillegg eller kun er nødvendig for faktureringsformål.

Trafikkdata som ikke er nødvendige for faktureringsformål skal slettes så snart som mulig etter at kommunikasjonen er avsluttet. For trafikkdata som stammer fra bruk av mobiltelefoner regnes kommunikasjonen som avsluttet i det brukeren bryter forbindelsen.

Trafikkdata som i tillegg eller kun er nødvendig for faktureringsformål kan lagres så lenge de er nødvendige, hvilket i praksis vil si inntil klagefristen er gått ut eller etter at rettslig tvist om kravet er avgjort.

Den adgang loven gir til å lagre trafikkdata er etter dette både innholds- og omfangsmessig i samsvar med konsesjonsvilkårene. Fordi lovens her ikke går lenger enn, eller begrenser, de regler som følger av konsesjonen, gjelder de nærmere vilkår som for øvrig er satt i konsesjonen som følge av lex specialis prinsippet. Dersom det kommer en endring i lov eller konsesjon som gjør at disse ikke lenger stemmer overens, vil derimot loven gå foran konsesjonen.

Av ekomloven § 2-7 andre ledd, siste setning, fremgår det dessuten at samtykke er et eget grunnlag for ”annen behandling av trafikkdata”. I flg. Ot.prp. nr. 58 (2002-2003), side 92, menes med dette ”enhver bruk av trafikkdata, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter”. Fordi trafikkdata er personopplysninger må dette sees på bakgrunn av definisjonen av behandling av personopplysninger i personopplysningsloven § 2, nr. 2, og samtykke etter ekomloven må dessuten være gitt ihht. vilkårene i personopplysningsloven § 2, nr. 7. Se pkt. 5.2.4 om samtykke som grunnlag for utlevering av trafikkdata til politiet.

Tredje ledd inneholder hjemmel for at myndighetene kan gi forskrift om forhold regulert i første og annet ledd. Ekomforskriften inneholder ingen slike regler av betydning for denne oppgaven.

2.1.3 Ekomloven § 2-8 - Tilrettelegging for lovbestemt tilgang til informasjon

Ekomloven § 2-8 første ledd pålegger teleoperatører og tilbydere av teletjenester plikt til å tilrettelegge nett og tjenester slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres. Omfanget av denne tilretteleggingsplikten er i Ot.prp. nr. 58 (2002-2003), side 93, beskrevet som ”kommunikasjonskontroll som gjennomføres av politiet etter reglene i straffeprosessloven kapittel 16a” og dessuten ”oppfylling av utleveringspålegg etter strprl. § 210 når utleveringspålegget gjelder informasjon om sluttbruker og elektronisk kommunikasjon.” En naturlig tolking av ordlyden i § 2-8 innebærer dog at tilretteleggingsplikten gjelder *enhver* lovbestemt tilgang til trafikkdata, hvilket innebærer at tilretteleggingsplikten dessuten omfatter den informasjon som utleveres etter fritak fra taushetsplikten fra PT eller retten, etter samtykke eller nødrett og de data som beslaglegges etter nektet utlevering, jf. kap. 5. Noen plikt til å lagre trafikkdata kan derimot ikke tolkes inn i tilretteleggingsplikten i § 2-8. Inntil slik lagringsplikt eventuelt vedtas er derfor mengden av trafikkdata det finnes ”lovbestemt tilgang” til avhengig av hvilke data som lovlig kan lagres i medhold av Datatilsynets konsesjonsvilkår og ekomloven § 2-7, jf. pkt. 2.1.1 flg. Forskriftshjemmelen i § 2-7 tredje ledd, jf. ovenfor, må sees i sammenheng med formålet bak § 2-8.

For at formålet med kommunikasjonskontroll skal kunne oppnås tilfredsstillende er det i Ot.prp. nr. 58 (2002-2003), side 93, videre antatt at tilretteleggingsplikten innebærer et krav om den høyeste dekningsgrad som er teknisk mulig, og dessuten tekniske løsninger som medfører lavest mulig risiko for at kontrollen blir oppdaget.

Annet ledd fastsetter statens plikt til å betale teleoperatørens kostnader i forbindelse med oppfyllelsen av pliktene etter § 2-8. Praksis i dag er at operatørene fakturerer politiet pr. oppdrag.

Hjemmel til å gi forskrifter om gjennomføringen av tilretteleggingsplikten etter første ledd finnes i tredje ledd. Det er presisert at forskriftshjemmelen også omfatter rett til å fastsette lagringsplikt for trafikkdata i en bestemt periode. Ekomforskriften inneholder ingen regler om lagringsplikt for trafikkdata eller gjennomføringsplikten for øvrig. Spørsmålet om det burde innføres plikt til lagring av trafikkdata er behandlet i pkt. 3.4.

I Ot.prp nr. 58 (2002-2003), side 93, er det antatt at hjemmelen til å gi forskrift om plikt til lagring av trafikkdata, som følger av ekomloven § 2-8 tredje ledd, vil være aktuell å benytte dersom plikten til å slette eller anonymisere personopplysninger som følger av § 2-7 skulle vise seg å medføre at de forskjellige bestemmelser som hjemler lovbestemt tilgang til trafikkdata ikke kan gjennomføres. Med andre ord er forskriftshjemmelen gitt for å sikre at politiet og påtalemyndigheten minst får den tilgang til trafikkdata de trenger for å gjennomføre effektiv kontroll med disse. Det at ekomforskriften ikke innholder slike bestemmelser, kan sees som et uttrykk for at ekomloven § 2-7 tolkes slik at den ikke endrer teleoperatørenes plikter eller rettigheter etter konsesjonen, jf. pkt. 2.1.2. At lovgiver ikke brukte forskriftshjemmelen kan også sees som et uttrykk for at teleoperatørenes lagringspraksis ikke medfører at politiets muligheter til kontroll etter konsesjon og lovgivning er begrenset, slik at det ikke var behov for eller ønske om en endring. Et annet spørsmål er om teleoperatørenes lagringspraksis er i strid med loven, og om politiet fremdeles minst hadde fått den tilgang til trafikkdata de trenger for å gjennomføre effektiv kontroll med disse dersom konsesjonsvilkårene satt av Datatilsynet hadde vært fulgt. Disse spørsmålene er behandlet i pkt. 3.3 flg. og 3.4.

3 Teleoperatørenes lagringspraksis

Det er en viss forskjell i lagringspraksis mellom Telenor og Netcom. Dette skyldes dels forskjeller i tekniske løsninger og muligheter mellom de to selskaper, og dels ulike tolkninger og oppfølgninger av regelverket gitt i lover, forskrifter og konsesjon.

3.1 Telenor[11]

Hver gang en kunde bruker Telenors mobilnett til å ringe opp noen, bruke WAP, GPRS eller sender en SMS eller MMS, lagrer Telenor en ”fakturastreng”. Denne lagringen foregår på samme måte ved all utgående og inngående trafikk, uavhengig av om det er en av Telenors egne kunder, eller en kunde fra en annen teleoperatør som leier Telenors nett. En ”fakturastreng” er en rekke av informasjon for bruk til faktureringsformål. Telenors fakturastrenger inneholder informasjon om: Dato, klokkeslett for samtalens start og slutt, hvilket mobiltelefonnummer kommunikasjonen gikk til, hvilket land kommunikasjonen gikk til, hvilken basestasjon avsender var knyttet til på kommunikasjonstidspunktet, id på den sentralen eller cellen i basestasjonen avsender var knyttet til på kommunikasjonstidspunktet, om kommunikasjonen ble viderekoblet, IMEI-nummeret til håndsettet som ble brukt og om det aktuelle SIM-kortet var et tvillingkort[12].

For utgående samtaler blir fakturastrengene lagret i opptil tre eller fem måneder, avhengig av hvilket faktureringsmønster kunden har. De aller fleste kunder blir fakturert etterskuddsvis hver måned, og trafikkdataene lagres da i ytterligere to måneder før de rutinemessig blir slettet. For kunder som bare faktureres kvartalsvis, lagres dataene i opptil tre måneder før fakturering, og de samme to månedene etter fakturering før

[11] Informasjon om Telenors lagringspraksis er gitt i møte med Audun Tollum-Andersen, Director of Security, Telenor Mobil, den 02.02.04.

[12] Tvillingkort er et ”kopiert” SIM-kort abonnenten kan kjøpe slik at flere håndsett kan motta anrop til samme nummer, f.eks. dersom man har en fast mobiltelefon i bilen og en annen til å ta med seg.

sletting. Trafikkdata fra kontankorttkunder som har forhåndbetalt sitt abonnement blir lagret i 3 måneder.

I tillegg til utgående samtaler lagrer Telenor dessuten trafikkdata fra alle innkommende samtaler i 3 måneder.

Ved begjæring om utlevering av trafikkdata for et spesifikt telefon- eller IMEI-nummer får politi eller påtalemyndighet en tilpasset utskrift av disse for den aktuelle periode.

Klagefristen på en faktura fra Telenor går ut ved forfall.

3.2 Netcom[13]

Netcom lagrer også fakturastrenger hver gang en kunde bruker sin mobiltelefon til utgående eller inngående trafikk over deres mobilnett. Lagringen er uavhengig av hvilken tjenestetilbyder kunden har kjøpt sitt abonnement fra. Innholdet i fakturastrengen kan variere litt avhengig av hvilke tjenester bruken stammer fra, men med unntak av opplysninger om tvilling-SIM er Netcoms fakturastreng i hovedsak den samme som for Telenor. Når Netcom utleverer trafikkdata til politiet eller påtalemyndigheten, inneholder disse i tillegg navnet på den registrerte brukeren av det telefonnummeret kontrollen gjelder.

Netcoms lagringspraksis skiller seg fra Telenors ved at alle trafikkdata lagres i 5 måneder. Dette gjelder både den inngående og utgående trafikken. Med unntak av kontantkunder faktureres alle Netcoms privatkunder hver måned, og bedriftskunder hvert kvartal. Før vedtakelsen av ekomloven lagret Netcom alle trafikkdata i seks måneder, men denne praksisen ble lagt om på grunn endringer i konsesjonsvilkårene fra Datatilsynet.

Netcoms kunder har 15 dagers klagefrist på en mottatt faktura.

---

[13] Informasjon om Netcoms lagringspraksis er gitt i møte med Hilde Lombnæs, Juridisk Rådgiver, Sikkerhetsavdelingen, Netcom den 04.03.04.

3.3 Er teleoperatørenes lagringspraksis lovlig?

Spørsmålet om teleoperatørenes lagringspraksis er lovlig kan i likhet med redegjørelsen for innholdet i konsesjonen deles inn tidsmessig, etter hvor lenge trafikkdata lagres før sletting, og innholdsmessig, etter hvilke trafikkdata er omfattet av lagringen. Tidsmessig er teleoperatørenes rutiner forskjellige og behandles hver for seg. Innholdsmessig er lagringen i hovedsak den samme, og jeg behandler derfor begge selskaper under ett.

Konsekvensen av lagring i strid med konsesjon og lovgivning, er at politi og påtalemyndighet får adgang til store mengder informasjon som egentlig ikke skulle ha eksistert. Til tross for at dette innebærer en klar fordel fordi det bidrar til å løse en rekke kriminelle handlinger, tilsier sterke personverns- og rettssikkerhetsmessige hensyn innebærer at lagring må være i tråd med den gjeldende lovgivning.

Når jeg i det følgende snakker om teleoperatørenes lagringspraksis mener jeg den praksis som gjelder kunder som betaler til forfall, eller umiddelbart ved debitering av ringesaldo. Verken lov eller konsesjon begrenser hvor lenge operatørene kan lagre trafikkdata fra kunder som ikke gjør opp i rett tid.

3.3.1 Telenors praksis for sletting av data

Etter konsesjonen er det ikke grunnlag for å lagre trafikkdata fra samtaler som er gjort opp, utover eventuell klagefrist. Fordi klagefristen på en faktura fra Telenor løper ut ved forfall, medfører dette at Telenor plikter å slette trafikkdata fra kunder som betaler i tide senest på dette tidspunkt, jf. pkt. 2.1.1.2. For kunder som faktureres etterskuddsvis vil maksimal lovlig lagringstid dermed være henholdsvis en eller tre måneder avhengig av faktureringsmønsteret, ikke tre eller fem måneder slik som praksis er i dag.

Selskapet opplyser dog at dersom det oppstår tvist om beløpet vil klager behandles så lenge det finnes trafikkdata som kan belyse saken. Dette har den effekt at den i utgangspunktet ulovlige lagring som foregår etter klagefristens utløp, i praksis gjør at det eksisterer en uformell klagefrist på 60 dager. Siden en slik klagefrist er innenfor konsesjonens rammer, jf. pkt. 2.1.1.2, ville selskapets lagringsrutiner for slike kunder vært lovlig dersom klagefristen også formelt hadde vært 60 dager. Forutsatt at det på

grunnlag av Telenors praksis kan innfortolkes en 60 dagers klagefrist, er selskapets lagringspraksis overfor kunder som faktureres, tidsmessig i samsvar med konsesjonen.

For kunder som bruker kontantkort eller andre abonnement med forhåndbetalt ringetid (kontantkunder) forekommer det ingen etterskuddsvis fakturering, kun en debitering av ringesaldo umiddelbart etter at tjenesten er gjennomført. Dette gjelder også ved bruk av kontantabonnenter i utlandet. Fordi klagefristen løper ut ved forfall tilsier dette at Telenor ikke har lovlig adgang til å lagre trafikkdata fra kontantkunder i det hele tatt. En slik tolkning følger av konsesjonen pkt. 8, og dessuten direkte av ordlyden i ekomloven § 2-7, jf. pkt. 2.1.1.2 og 2.1.2. Dersom det kan innfortolkes en 60 dagers klagefrist på grunnlag av praksis, kan selskapet lovlig lagre trafikkdata fra kontantkunder i 60 dager. Telenors praksis med lagring av slike trafikkdata i 3 måneder kan uansett ikke sies å være i samsvar med konsesjonen.

Telenor lagrer også all inngående trafikk i tre måneder. Data fra inngående trafikk til abonnent som befinner seg i utlandet er faktureringsinformasjon, og Telenors lagringspraksis er dermed på dette området i samsvar med konsesjonen for kunder som faktureres kvartalsvis. For kunder som faktureres månedlig vil situasjonen være den samme for denne type inngående trafikk som for utgående trafikk, jf. ovenfor. Dersom den inngående samtalen kommer fra en abonnent som bruker Telenors nett vil trafikkdataene kunne lagres som øvrige utgående samtaler fra denne kunden, men ikke som trafikkdata for mottaker. Dersom den inngående samtalen derimot kommer fra abonnent som ikke bruker Telenors nett, er trafikkdata om denne abonnenten opplysninger som etter konsesjonens pkt. 8 og ekomloven § 2-7 kun kan anses som nødvendige for oppkobling eller gjennomføring av tjenesten. Slike data plikter teleoperatøren å slette når tjenesten er brutt, jf. pkt. 2.1.1.2 og 2.1.2.

3.3.2 Netcoms praksis for sletting av data

Netcom opererer med en klagefrist på fakturaer på 15 dager, og fakturerer alle bedriftskunder kvartalsvis og privatkunder hver måned. Selskapets praksis er videre å slette alle trafikkdata etter fem måneder, jf. pkt. 3.2. Denne praksis medfører at trafikkdata fra utgående samtaler, og trafikkdata fra inngående samtaler til Netcoms kunder i utlandet, for privatkunder lagres tre og en halv måned lenger enn fristene som

er fastsatt i konsesjonen. For bedriftskunder lagres de samme data en og en halv måned for lenge, jf. pkt. 2.1.1.2.

Lagring i fem måneder av trafikkdata fra inngående samtaler fra Norge vil være ulovlig, dersom de kommer fra kunder fra Telenors nett, og må ellers betraktes som utgående trafikk for den aktuelle kunde, jf. pkt. 3.3.1.

For kontantkundene kan Netcom etter konsesjonen lovlig lagre dataene i 15 dager inntil klagefristen har gått ut. Selskapets praksis medfører følgelig at disse lagres i fire og en halv måned utover konsesjonens rammer.

3.3.3 Innholdet i teleoperatørenes lagringspraksis

Som jeg har redegjort for tidligere i pkt. 2.1.1.2 og 2.1.2 kan trafikkdata ikke lagres for andre formål enn fakturering. Grunnlaget for fakturering av en mobiltelefontjeneste varierer litt mellom de forskjellige teleoperatører og abonnementer. De forskjellige momenter som inngår i faktureringen er i hovedsak samtalens varighet, hvilke(n) teleoperatør(er) kommunikasjonen gikk mellom og når på døgnet kommunikasjonen fant sted. Til forskjell fra det som er hovedregelen for fasttelefoni påvirker det ikke faktureringen hvor i landet en mobiltelefon befinner seg på kommunikasjonstidspunktet. Følgelig er det relevant å spørre om det av faktureringshensyn er nødvendig for teleoperatørene å lagre posisjonsdata, nærmere bestemt basestasjonsid og celle- eller sentralid.

Teleoperatørenes begrunnelse for slik lagring er at posisjonsdata er viktig dersom kunder påstår at det er feil i faktureringen, typisk ved å hevde at de ikke har brukt telefonen i slik utstrekning som fakturaen tilsier. Når teleoperatøren da ved hjelp av posisjonsdata kan påvise at alle samtalene for eksempel ble foretatt via den basestasjonen som ligger nærmest abonnentens bopel eller arbeidsplass, vil dette åpenbart bidra til å styrke teleoperatørens sak. At dette er en praktisk mulighet for teleoperatørene, som gjør det enklere å drive inn penger i saker hvor abonnenten nekter å betale, er det ingen tvil om. Spørsmålet er om disse dataene oppfyller vilkåret om nødvendighet for selve faktureringen. Problemstillingen kan deles ved å skille mellom posisjonsdata som angir basestasjon og data som angir celle- eller sentralid. De

sistnevnte gir en langt mer nøyaktig geografisk plassering, i det de angir hvilken sektor innenfor en basestasjons rekkevidde kommunikasjonen kom fra, jf. pkt. 4.5.

Utgangspunktet er at posisjonsdata ikke påvirker innholdet i faktureringen, og de kan derfor ihvertfall ikke sies å være umiddelbart nødvendige for denne. På den annen side kan det argumenteres for at fakturering også må innebære en mulighet til dokumentering og oppfølging av de fakturaer det oppstår strid om, ellers ville faktureringen i noen tilfeller kanskje vise seg å være verdiløs fordi teleoperatøren ikke får drevet inn pengene sine.

De beste grunner taler for at det avgjørende må være hva som kreves for at det skal anses bevist at en kunde har brukt sin mobiltelefon slik som teleoperatøren hevder. Dette vil i ytterste konsekvens føres som en sivil sak for retten, hvor det mest sannsynlige[14] alternativet normalt vil legges til grunn. Teleoperatørene vil, bortsett fra posisjonsdata, kunne legge frem samledata som inneholder opplysninger om bl.a. tidspunktet for den påståtte kommunikasjonen, hvem den gikk til og hvor lenge den varte. Videre må det kunne legges til grunn at trafikkdata produseres helt automatisk, og kun i forbindelse med at det aktuelle abonnement faktisk blir brukt. Muligheten for feilregistreringer er meget liten. Teleoperatørene må dessuten som hovedregel antas å ikke ha noen interesse i å lure sine kunder ved å jukse med tallene, og det må derfor bli opp til abonnenten å føre bevis for at det har skjedd en teknisk feil, eller at en tredjepart har klart å misbruke systemet slik at abonnenten urettmessig har blitt belastet for andres bruk.

I de aller fleste tilfeller må det antas at dokumentasjon bestående av samledata alene vil være tilstrekkelig fra teleoperatørenes side for å vinne slike saker. Dersom det hevdes å ha skjedd en teknisk feil eller påvirkning fra tredjemann, vil man uansett ikke uten videre kunne legge posisjonsdata til grunn som sikkert bevis. Den feil eller påvirkning som har skjedd kan jo like gjerne medføre feil i posisjonsdata som samledata.

[14] Jf. Rt. 1992 s. 64 ”P-pilledom II”

På dette grunnlag kan posisjonsdata, informasjon om hvilken basestasjon og hvilken sektor eller celle i denne kommunikasjonen var knyttet til, etter min oppfatning ikke sies å være avgjørende for faktureringsformål. Fordi slike data heller ikke oppfyller noen av de øvrige formålene i konsesjonen, jf. pkt. 2.1.1.1, mener jeg slik lagring faller utenfor konsesjonens og lovens rammer. I lys av den store praktiske betydning slike data har, og hvor viktig det vil være for politi og påtalemyndighet å få tilgang til slik informasjon, er uttrykkelig hjemmel for lagring og bruk av posisjonsdata etter min oppfatning den beste løsningen. Et alternativ er å utvide definisjonen av hvilke trafikkdata som kan lagres i konsesjonen og ekomloven § 2-7, slik at dette ikke bare omfatter informasjon som er nødvendig til faktureringsformål.

3.4 Burde vi ha plikt til å lagre trafikkdata?

Spørsmålet om plikt til å lagre trafikkdata er nylig tatt opp både i forbindelse med vedtakelsen av ekomloven, ekomforskriften og av Politimetodeutvalget i NOU 2004:6. Når Datakrimutvalgets andre delutredning foreligger vil de sannsynligvis også ha tatt stilling til dette vanskelige spørsmålet.

Verken ekomloven eller ekomforskriften inneholder regler om lagring av trafikkdata, men det er åpnet for å gi slik plikt i forskrift, jf. ekomloven § 2-8, tredje ledd. Som jeg var inne på i pkt. 2.1.2 er det i Ot.prp. nr. 58 (2002-2003), side 93, uttalt at det vil være aktuelt å benytte denne forskriftshjemmelen dersom plikten til å slette eller anonymisere personopplysninger som følger av § 2-7 skulle vise seg å medføre at bestemmelsene i blant annet strprl. kap. 16 a om kommunikasjonskontroll, og andre bestemmelser som hjemler lovbestemt tilgang til informasjon, ikke kan gjennomføres.

Som det fremgår av min vurdering av forholdet mellom teleoperatørenes lagringspraksis, og de rammer som er satt for denne i Datatilsynets konsesjon og ekomloven kapittel 2 i pkt. 3.3 flg., syntes den lovbestemte tilgang til trafikkdata å være i dårlig samsvar med den tilgang som faktisk forekommer. Dersom Datatilsynets konsesjonsvilkår og plikten til å slette trafikkdata etter ekomloven § 2-7 hadde blitt fulgt opp i praksis, er det etter min mening tvilsomt om bestemmelsene i straffeprosessloven kap. 16b, eller de øvrige bestemmelser som hjemler lovbestemt tilgang til trafikkdata,

kunne gjennomføres. Jeg mener derfor at det i dag foreligger en slik situasjon som beskrevet i Ot.prp. nr. 58 (2002-2003), side 93.

Flertallet på tre i Politimetodeutvalget foreslår i NOU 2004:6, side 210, å innføre lagringsplikt for trafikkdata i ett år for på nærmere vilkår å kunne gjennomføre preventiv kontroll av trafikkdata (kontroll for å avverge kriminalitet på grunnlag av berettiget mistanke om at spesifikke personer kommer til å begå nærmere bestemte lovbrudd, jf. NOU 2004:6, side 171 flg.). Flertallet finner det uholdbart at lagring av trafikkdata, som allerede i dag viser seg å være av uvurdelig betydning for moderne politiarbeid, ensidig skal være bestemt av personvernhensyn. Forslaget innebærer bl.a. at dataene skal lagres hos teleoperatør, og at utlevering skal foregå etter samme mønster som i dag. Dette skal etter flertallets oppfatning begrense de personvernmessige betenkeligheter ved å lagre slike enorme mengder data, og hensynet til en effektiv kriminalitetsbekjempelse må derfor veie tyngre når de personvernmessige hensyn er ivaretatt.

Mindretallet, på side 210-211, peker på at trafikk- og posisjonsdata først ble en aktuell politimetode da den tekniske utvikling åpnet for slike muligheter. Metoden var den gang ikke gjenstand for en debatt om de grunnleggende personvernspørsmål den reiser. Etter mindretallets oppfatning er flertallets vurdering av disse hensynene ikke grundige nok til å legitimere forslaget. Videre peker mindretallet på misbrukspotensialet ved lengre tids lagring, ikke bare fra politiet. Flertallet har ikke vurdert sikkerheten rundt teleoperatørenes lagringsmuligheter. Avslutningsvis peker mindretallet på at regulering av lagringstid ikke burde plasseres i politiloven, men at dette heller hører hjemme i ekomloven hvor det også er gitt forskriftshjemmel til å regulere spørsmålet. Lagringsplikt for trafikkdata faller dessuten utenfor Politimetodeutvalgets mandat og vurderingen burde overlates til Datakrimutvalget i deres andre delutredning.

Jeg mener lagringsplikt som skissert av flertallets i Politimetodeutvalgets forslag i utgangspunktet har mye for seg. Lagring av dataene hos teleoperatør, som må forutsettes å oppfylle de strengeste krav til sikkerhet i forhold til både internt misbruk og elektroniske angrep utenfra, jf. ekomloven § 2-7 første ledd og pkt. 2.1.2, vil etter

min oppfatning være en tilfredsstilende løsning på de personvernmessige problemstillinger forbundet med slik lagring.

I forhold til plasseringen av hjemmel til slik lagringsplikt i politiloven er jeg enig med mindretallet om at denne neppe er helt heldig. Ekomloven § 2-8 tredje ledd, jf. pkt 2.1.3, gir departementet hjemmel til å fastsette lagringsplikt i forskrift, og ekomforskriften eller ekomloven selv må sies å være de best egnede sted for lovfesting av dette. Uansett plassering vil det etter min oppfatning som sagt være lite hensiktsmessig å ha en egen hjemmel for lagring ifm. preventiv kontroll av trafikkdata. Hvordan lagrede data skal brukes bør ikke være avgjørende for hvor lagringsplikten eventuelt skal hjemles. En egen hjemmel for lagringsplikt i ekomloven, ved siden av en eventuell separat hjemmel for preventiv kontroll i politiloven, vil etter min mening være den beste løsning.

I lys av at den gjeldende rettsoppfatning i Europa går mot å tillate lengre lagring av trafikkdata, og at den samfunnsmessige gevinst ved å kunne bruke dette i bekjempelsen av kriminalitet etter min mening overstiger de personvernmessige betenkeligheter dersom lagring gjennomføres slik som foreslått, mener jeg teleoperatørene bør gis plikt til lagring av trafikkdata i ett år. Dagens lovgivning setter ingen tidsmessige begrensninger for hvor langt bakover politi og påtalemyndighet kan gis anledning til å foreta kontroll med historiske trafikkdata. Det vil derfor ikke i utgangspunktet være behov for noen ytterligere lovendringer etter at eventuell lagringsplikt er vedtatt. Slik begrensning bestemmes konkret for hvert tilfelle av PT eller retten, i forhold til begjæringen og innenfor rammene av hvor gamle data som er tilgjengelige og det aktuelle hjemmelsgrunnlag, jf. kapittel 5.

4 Bruk av trafikkdata i praksis[15]

4.1 Innledning

PT behandlet i 2003 ca. 1700 begjæringer fra politiet om unntak fra den lovbestemte taushetsplikt etter ekomloven § 2-9. I tillegg kommer en betydelig mengde saker som ikke behandles av PT, dvs. saker hvor abonnenten har gitt sitt samtykke, nødrettssaker hvor politiet tar direkte kontakt med teleoperatøren og saker som avgjøres av retten etter straffeprosessloven § 118 annet ledd eller § 216b annet ledd, bokstav c. Av disse er det kun samtykke- og nødrettssakene som utgjør noen mengde av betydning. Med hjemmel i kommunikasjonskontrollforskriften § 10 annet ledd rapporterer Riksadvokaten årlig politiets bruk av kommunikasjonskontroll i medhold av straffeprosessloven kap. 16a til Justisdepartementet. Rapporten inneholder bl.a. informasjon om antall saker og hva slags type kontroll som er benyttet. Fordi rapporten er gradert strengt fortrolig er det ikke mulig for meg å si noe sikkert om omfanget av kontroll med trafikkdata etter straffeprosessloven § 216b annet ledd, bokstav c. På bakgrunn av informasjon fra teleoperatørene er det likevel klart at reglene om kommunikasjonskontroll generelt sett benyttes svært sjelden, og i særlig grad gjelder dette hjemmelen for utlevering av trafikkdata.

Totalt er omfanget av kontroll av trafikkdata meget betydelig, og sterkt stigende. I løpet av de to første måneder i 2004 behandlet PT mellom 300 og 400 saker, noe som tilsier mer enn en fordobling av saksmengden fra i fjor dersom utviklingen fortsetter. Til tross for at Telenor er den teleoperatøren med flest mobilkunder, er fordelingen av antall saker om kontroll med trafikkdata mellom Netcom og Telenor relativt lik. Grunnen til at

[15] Teknisk og praktisk informasjon om politiets bruk av trafikkdata er gitt i møter med Audun Tollum-Andersen, Director of Security, Telenor Mobil, den 02.02.04, Hilde Lombnæs, Juridisk Rådgiver, Sikkerhetsavdelingen, Netcom den 04.03.04 og Asle Fuhr, Odd Martin Helleland og Kjerstin Ringdal i Post- og teletilsynet den 11.03.04.

forskjellen er mindre enn antallet kunder skulle tilsi er antakelig at Netcom har en betydelig mengde uregistrerte kontantabonnenter. Dette er en abonnementstype som er spesielt populær blant individer som ønsker å unndra seg, og er særlig utsatt for, kontroll.

Et viktig poeng ved bruk av trafikkdata fra mobiltelefoner er at denne alene ikke med sikkerhet kan identifisere hvem som faktisk benytter seg av den overvåkede telefonen. Man kan kun si i hvilket navn de aktuelle håndsett og telefonnummer er registrert på, bortsett fra i de tilfeller det dreier seg om uregistrerte kontantkortkunder.

På grunn av denne usikkerheten er trafikkdata alene neppe tilstrekkelig til å bevise skyld i en straffesak, uavhengig av hvilket hjemmelsgrunnlag som ligger til grunn for kontrollen. I den mye omtalte Baneheia-saken[16] var bruk av trafikkdata et av påtalemyndighetens viktigste tekniske bevis, men denne saken er et godt eksempel på hvordan trafikkdata bare utgjør en del av bevismaterialet mot personer som er siktet for alvorlige kriminelle handlinger. Dersom man med sikkerhet skal knytte trafikkdata til en person må dette benyttes i sammenheng med kommunikasjonsavlytting etter straffeprosessloven § 216a. Uten tilståelse er det i øvrige saker umulig å få bekreftet hvem som benyttet en telefon på et gitt tidspunkt.

Til tross for den grad av usikkerhet som alltid vil være knyttet til bruk av trafikkdata er dette likevel et meget verdifullt verktøy i forbindelse med etterforskning. Trafikkdata vil i de fleste tilfeller gå langt i å skape skjellig grunn til mistanke i forbindelse med for eksempel spørsmål om varetektsfengsling for det forhold kontrollen gjelder.

Avhengig av hvilke behov politiet har for informasjon fra trafikkdata, og hvilke muligheter for innhenting som foreligger i den konkrete sak, vil både innhold og bruksområde for de data som hentes inn variere. Som jeg var inne på i pkt. 1.2.1 deles trafikkdata fra mobiltelefoner først inn etter når de oppsto i forhold til tillatelsen til kontroll, altså om de er historiske eller fremtidige. Kontroll med historiske trafikkdata

[16] Kristiansand byrett (nå tingrett) nr. 01-00374. Anke over straffutmåling og bevis til Agder Lagmannsrett, LA-2001-000980.

utgjør den klart største delen av politiets bruk. Videre kan både historiske og fremtidige trafikkdata deles inn i samle- og posisjonsdata. Jeg skal i det følgende redegjøre for og vurdere polities bruk av de forskjellige typer trafikkdata

4.2 Historiske samledata

Historiske samledata kan utleveres på grunnlag av alle aktuelle hjemler, jf. kap. 5. Slike data brukes av politiet for å dokumentere hvilke personer en mistenkt har vært i kontakt med, til hvilke tidspunkter og hvor lenge samtalene har vart. Personene identifiseres ved hjelp av telefonnummeret deres, eller ved hjelp av håndsettets IMEI-nummer dersom dette er kjent. Fordi mange kriminelle benytter seg av uregistrerte forhåndsbetalte abonnementer, og det ikke er uvanlig at de disponerer opp til fem eller ti forskjellige abonnementer og håndsett, er det ofte vanskelig å danne seg et fullstendig bilde av en enkelt mistenkts kommunikasjon. I slike tilfeller er metodene SIM- eller IMEI-søk svært verdifulle (jf. pkt. 1.2.1).

4.3 Historiske posisjonsdata

Historiske posisjonsdata kan utleveres med hjemmel i alle grunnlag som åpner for utlevering av trafikkdata, jf. kap. 5. De historiske posisjonsdata er informasjonen fra fakturastrengen om hvilken basestasjon, og hvilken sentral eller celle i denne, en mobiltelefonen var knyttet til på samtaletidspunktet. Ved hjelp av denne informasjonen kan politiet følge en telefons bevegelser så langt bakover som det finnes lagrede data, i de fleste tilfeller 3 eller 5 måneder (se pkt. 3.1 og 3.2 om lagringspraksis). Denne metoden gjør at politiet for eksempel kan finne ut om en konkret mistenkt (eller i det minste mobiltelefonen hans) var i nærheten av åstedet da den kriminelle handling ble begått, og på den måten styrke eller svekke mistanken mot vedkommende. Avhengig av den spesifikke basestasjonens rekkevidde, og hvor stor sektor denne sender signaler i, vil nøyaktigheten av den geografiske plasseringen fra historiske posisjonsdata variere veldig. Basestasjoner har rekkevidder fra opp til 120 kilometer i åpne områder, og ned til 50 meter i bykjerner. Bare i Oslo sentrum finnes flere tusen basestasjoner, og historiske posisjonsdata herfra gir ofte en svært nøyaktig plassering.

Historiske trafikkdata benyttes også i det som kalles basestasjonsøk eller masteinfo. Disse metodene innebærer at teleoperatørene sorterer ut trafikkdata slik at politiet får

informasjon om hvilke SIM- og IMEI-numre som på et gitt tidspunkt ble registrert i et bestemt område (for eksempel Karl Johans gate mellom Stortinget og Slottet fra kl. 00:30-01:00 torsdag 04.03.04). I tilfeller hvor det er begått en alvorlig kriminell handling kan politiet raskt få en liste over personer som kan ha vært innblandet i episoden, eller sitte på verdifulle vitneopplysninger. Bruken av basestasjonsøk er problematisk i forhold til spesifikasjonskravet i straffeprosessloven § 216b (jf. pkt. 5.3.3), og kan derfor ikke lovlig benyttes dersom kontrollen av trafikkdata er hjemlet i straffeprosessloven kap. 16a. I praksis utgjør denne begrensningen likevel ikke noe problem fordi basestasjonsøk kan gjennomføres med hjemmel i de øvrige grunnlag for kontroll med trafikkdata. Rettssikkerhetsmessig er det dog betenkelig at det ikke er sammenheng mellom hvor strenge vilkår som stilles for bruk av et tvangsmiddel, og hvilken rekkevidde det har. PT opphever normalt taushetsplikten ved begjæring om basestasjonssøk. Slike saker utgjør ca. 20% av det totale antall saker teleoperatørene behandler.

Spørsmålet om teleoperatørene etter dagens konsesjon og lovgivning i det hele tatt har anledning til å lagre posisjonsdata er drøftet i pkt. 3.3 flg.

4.4 Fremtidige trafikkdata

Fremtidige trafikkdata skiller seg ikke fra historiske trafikkdata på noen annen måte enn at de er nyere, men til forskjell fra historiske data kan de bare utleveres etter samtykke eller kjennelse begrunnet i straffeprosessloven § 216b, jf. pkt. 5.2.4 og 5.3.3. Også fremtidige data kan deles inn i samledata og posisjonsdata, og bruksområdene er de samme som for historiske data. Begrepet fremtidige trafikkdata er litt misvisende fordi det naturligvis ikke oppstår noen trafikkdata før kundene bruker sine mobiltelefoner. Det er i realiteten snakk om oppdaterte data, i stedet for gamle data som hentes ut fra en database. Det fremtidige kommer av at retten på forhånd kan avsi kjennelse om utlevering av slike data som forventes å ville oppstå i fremtiden. I praksis sender teleoperatørene slike oppdaterte trafikkdata til politiet etter avtale, forutsatt at dette ligger innenfor rammen av kjennelsen, jf. pkt. 5.3.3.

4.5 Trafikkdata i sanntid

En spesiell form for trafikkdata er data som produseres og analyseres i sanntid. Ved hjelp av slike trafikkdata kan teleoperatørene spore opp en mobiltelefon på grunnlag av kontinuerlig oppdaterte og mer utfyllende posisjonsdata. Fordi bruk av slike data er mer inngripende enn de øvrige kan slik kontroll kun skje med hjemmel i straffeprosessloven § 216b eller nødrett, jf. pkt. 5.3.3 og 5.2.5. Samtykke er ikke praktisk. Metoden fungerer slik at teleoperatøren sender ut en skjult tekstmelding til den mistenktes håndsett. Trafikkdata fra denne tekstmeldingen, som er umulig å oppdage for mottakeren, kommer umiddelbart tilbake til operatøren. Ved hjelp av de innkomne posisjonsdata plasseres mistenktes håndsett geografisk, og metoden kan gjentas kontinuerlig for å følge mistenktes bevegelser. Slike opplysninger skiller seg dermed fra de "tradisjonelle" trafikkdata ved at opplysningene om abonnenten provoseres frem, i stedet for å basere seg på abonnentens ordinære bruk av mobiltelefonen.

Fordi det ikke er snakk om trafikkdata basert på abonnentens egen mobiltelefonbruk, men trafikkdata generert av skjulte tekstmeldinger sendt med det formål å spore opp vedkommende, er det nærliggende å trekke en parallell til tvangsmidlet teknisk sporing i straffeprosessloven kap. 15a. I begge tilfeller er det snakk om å spore mistenkte ved hjelp av signaler påtalemyndigheten provoserer frem. Forskjellen ligger i at dersom politiet etter § 202c bokstav a skal plassere teknisk peileutstyr på klær eller gjenstander som den mistenkte bærer på seg, som for eksempel vedkommendes mobiltelefon, stilles det vesentlig strengere vilkår. Slik sporing forutsetter skjellig grunn til mistanke om en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i ti år eller mer, eller som rammes av lov 18. desember 1987 nr. 93 om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. (eksportkontrolloven) § 5. Sporing ved hjelp av trafikkdata i sanntid kan etter straffeprosessloven § 216b første ledd bokstav a benyttes dersom minste strafferamme er fengsel i fem år, og i tillegg i enkelte andre spesielle tilfeller etter første ledd bokstav b hvor strafferammen er enda lavere, jf. pkt. 5.3.3. Forholdsmessighetsvurderingen som må foretas i begge tilfeller må antas i hovedsak å være den samme, jf. pkt. 5.3.1. Som redegjørelsen nedenfor viser må sporing ved bruk av trafikkdata i sanntid i stor utstrekning sies å være like inngripende som teknisk sporing.

Ved sporing i sanntid tar en utgangspunkt i hvilken basestasjon abonnenten er knyttet til. Dette forteller mer eller mindre nøyaktig hvor i landet abonnenten befinner seg. Hvor nøyaktig plasseringen er avhenger av hvor lang rekkevidde basestasjonen har, og hvor stor sektor signalene fra basestasjonen dekker. I utgangspunktet sender alle basestasjoner signaler 360 grader utover fra sin posisjon, slik at mistenkte i prinsippet kan befinne seg i en hvilken som helst retning innenfor signalenes rekkevidde som er opp til 120 km. fra basestasjonen. På grunn av geografisk blokkering av signaler (for eksempel fra fjell eller bygninger) sender likevel de fleste basestasjoner i realiteten bare ut signaler i en mindre sektor og kortere avstander. Mange basestasjoner er også delt inn i flere sentraler, eller såkalte celler, som sender signaler i hver sin sektor. Celle- eller sentralid er en del av de trafikkdata som lagres i en fakturastreng, og bidrar til å spesifisere håndsettets geografiske posisjon. Ved sporing i sanntid vil en dessuten benytte seg av såkalte tidsluker, en metode som for enkelthets skyld kan beskrives som en oppbrytning av signalene ved for eksempel å bare sende på hver andre eller tredje tidsenhet. Ved hjelp av disse kan operatøren i tillegg beregne hvor lang tid det tar før signalene kommer tilbake til basestasjonen. På den måten kan en avgjøre avstanden mellom basestasjonen og håndsettet. Når en vet hvilken sektor den aktuelle basestasjon sender i, og i tillegg hvor stor avstanden er fra basestasjonen til håndsettet, kan sporing bli svært effektiv selv i strøk med betydelige avstander fra stasjon til stasjon.

Uavhengig av hvordan man vurderer forholdet mellom hvor inngripende teknisk sporing og sporing ved hjelp av trafikkdata i sanntid er, syntes det klart at den siste metoden har et betydelig større anvendelsesområde. Sporing med trafikkdata i sanntid kan benyttes over alt hvor det er mobildekning, og fordi man ikke er avhengig av å plassere en sender er den dessuten vesentlig enklere å benytte seg av. Det fremstår som betenkelig at to metoder for sporing, som på mange måter må sies å være minst like inngripende og effektive, har så forskjellige kriterier for anvendelse. Av hensyn til oppgavens omfang kan jeg dessverre ikke gå nærmere inn på forskjellene mellom disse former for sporing.

5 Hjemmelsgrunnlag for bruk av trafikkdata

5.1 Innledning

Trafikkdata er ihht. ekomloven § 2-9 første ledd taushetsbelagte opplysninger, jf. pkt. 5.1.1. For at politiet likevel skal få tilgang til disse kreves enten unntak fra taushetsplikten, eller annen hjemmel som tillater utlevering til tross for at taushetsplikten ikke på forhånd er opphevet (og som dermed i seg selv opphever taushetsplikten). Unntaksmessig er dette grunnlaget bruk av et straffeprosessuelt tvangsmiddel, men i de fleste tilfeller er utlevering av trafikkdata basert på annen hjemmel.

Det klart vanligste er utlevering på grunnlag av fritak fra taushetsplikten. Spørsmålet om politiet kan få innsyn i trafikkdata er derfor i de fleste tilfeller et spørsmål om PT gir tillatelse til unntak fra den lovbestemte taushetsplikten i ekomloven § 2-9. Uavhengig av om PT fritar teleoperatøren fra taushetsplikten eller ikke, kan retten ved kjennelse overprøve avgjørelsen. Videre gjelder ikke taushetsplikten overfor den dataene gjelder, og dersom abonnenten samtykker til utlevering trenger følgelig ikke PT vurdere saken. PT får heller ikke saken inn til vurdering dersom utleveringsbegjæringen er begrunnet i nødrett, i det politiet da henvender seg direkte til teleoperatøren.

Alternativet til disse grunnlag er at utleveringen skjer i form av et straffeprosessuelt tvangsmiddel. De aktuelle metoder er beslag eller utleveringspålegg, dersom teleoperatøren nekter å forklare seg til tross for at PT har fritatt fra taushetsplikten, eller utlevering som følge av reglene om kommunikasjonskontroll. Tidligere forlangte teleoperatørene alltid rettens kjennelse for å utlevere trafikkdata, og hovedregelen var da at utlevering skjedde som følge av et utleveringspålegg. I dag utleverer teleoperatørene i praksis alltid trafikkdata når de er fritatt fra taushetsplikten, og reglene om beslag og utleveringspålegg brukes svært sjelden. Ved lovendring i 1992 ble det lagt til et nytt kapittel 16a om kommunikasjonskontroll i straffeprosessloven. Etter siste lovendring i 1999 finnes det i § 216b hjemmel for kontroll av trafikkdata på grunnlag av rettens

kjennelse, uten at PT på forhånd har vurdert fritak. Hjemmelen for utlevering av trafikkdata etter denne regelen brukes også svært sjelden, og i praksis kun i forbindelse med andre former for kommunikasjonskontroll.

5.1.1 Ekomloven § 2-9 - Taushetsplikt

Som nevnt ovenfor er trafikkdata underlagt taushetsplikt, og det kreves derfor et særskilt grunnlag for at slike opplysninger likevel skal kunne utleveres. Taushetsplikten følger av ekomloven § 2-9 første ledd, som bestemmer at tilbyder og installatør plikter å bevare taushet om innholdet av elektronisk kommunikasjon, og andres bruk av elektronisk kommunikasjon. Fordi trafikkdata er uavhevgig av innholdet i kommunikasjonen, jf. pkt. 1.2.1, faller trafikkdata inn under begrepet ”bruk av elektronisk kommunikasjon”.

Straffeprosessloven § 2-9 tredje ledd presiserer at taushetsplikten ikke er til hinder for at teleoperatørene opplyser påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Dette er ikke opplysninger som faller inn under definisjonen av trafikkdata, jf. pkt. 1.2, fordi de er faste opplysninger fra teleoperatørenes kunderegistre om telefonnumre, abonnementsdetaljer etc., og ikke er resultat av den konkrete bruken av mobiltelefoner. Telefonnumre kan likevel være underlagt taushetsplikt som følge av avtale om hemmelig telefonnummer, men slike avtaler gjelder ikke overfor politiet. Hvilke opplysninger som faller inn under unntaket fra taushetsplikten er vurdert i Ot.prp. nr. 58 (2002-2003), side 93 og 94, hvor det tas til orde for en utvidende tolkning som inkluderer blant annet SIM- og IMEI-nummer. Fordi slike opplysninger i denne sammenheng ikke er å anse som trafikkdata faller en grundigere redegjørelse for § 2-9 tredje ledd utenfor rammene av denne oppgaven.

5.2 Utlevering av trafikkdata uten bruk av tvangsmidler

Utlevering av trafikkdata uten bruk av tvangsmidler er den store hovedregel. Prosessøkonomisk er dette gunstig fordi det som regel ikke innebærer en avgjørelse fra retten, og fordi behandlingstiden i de fleste tilfeller er relativt kort. Rettssikkerhetsmessig kan det derimot være et problem at trafikkdata som regel kommer på politiets eller påtalemyndighetens hender, uten at abonnenten får den

beskyttelse som ville ha fulgt av loven dersom det lå et straffeprosessuelt tvangsmiddel til grunn for utleveringen.

5.2.1 Frivillig utlevering etter fritak fra taushetsplikten

Utlevering av trafikkdata innebærer etter straffeprosesslovens ordning en forklaring, og fordi teleoperatørene ikke er siktet eller mistenkt i saken får de status som vitne. Hovedregelen om vitneforklaringer er etter straffeprosessloven § 108 at enhver har vitneplikt for retten, med mindre noe annet er bestemt ved lov. Unntak finnes i straffeprosessloven § 118, som bestemmer at retten ikke kan motta forklaring fra vitne som har taushetsplikt som følge av tjeneste eller arbeid for bl.a. tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste. Slik taushetsplikt for teleoperatørene følger som tidligere nevnt av ekomloven § 2-9, jf. pkt. 5.1.1. Videre følger det av straffeprosessloven § 230 at heller ikke politiet har adgang til å oppta slik forklaring, og at politiet uansett ikke kan pålegge noen å forklare seg.

Unntak finnes i straffeprosessloven § 118 første ledd, jf. § 230 annet og tredje ledd, som bestemmer at departementet kan gi samtykke til at teleoperatører og deres ansatte kan avgi forklaring for retten eller politiet. Denne myndigheten ble delegert til PT den 15. september 1995, og ved brev av 14. desember 1995. Da taushetsbestemmelsene i telegrafloven av 29.april 1899, med virkning fra 1. januar 1996 ble overført til teleloven, videreførte departementet delegeringsvedtaket i brev av 5. mars 1996. Det er foreløpig ikke foretatt ytterligere videreføring av delegasjonen etter vedtagelsen av den nye ekomloven, hvilket medfører at PT inntil videre ikke har formell kompetanse til å gi slikt samtykke[17]. Slik kompetansemangel er betegnet som en personell kompetansemangel[18], og kan etter omstendighetene medføre at PTs vedtak er ugyldige. For at slike kompetansemangler skal medføre ugyldighet kreves det i tillegg at feilen kan ha virket inn på innholdet, jf. prinsippet i lov om behandlingsmåten i

[17] Det har ikke lyktes meg å få se vedtaket av 5. mars 1996. Dersom dette knytter PTs kompetanse til straffeprosessloven § 118, og ikke taushetsbestemmelsene i teleloven, medfører ikke den nye ekomloven brudd på hjemmelsrekken. På grunn av departementets tidligere praksis med hjemmlesoverføring på grunnlag av endringer i taushetsbestemmelsene, forutsetter jeg at brevet av 5. mars 1996 gir kompetanse overfor teleloven.

[18] Eckhoff 1997, s. 574.

forvaltningssaker (forvaltningsloven) 10. februar 1967, § 41. Fordi bruddet i hjemmelsrekken må antas å være midlertidig, og kun har oppstått som følge av lovendringen sommeren 2003, taler dette for at PTs vedtak i slike saker neppe kan sies å være ugyldige.

Følgen av at PT fritar teleoperatøren fra taushetsplikten er at denne får vitneplikt overfor retten og anledning til å forklare seg for politiet.

Reglene om vitneforklaring bærer preg av å være tilpasset en tid da en person kom ned til politiet og forklarte seg om de data begjæringen ba om, og dette var praksis i begynnelsen. I dag er prosessen den at politiet sender en begjæring pr. telefax til PT om å frita en teleoperatør fra taushetsplikten etter ekomloven § 2-9, med redegjørelse for mistanke om et straffbart forhold. Begjæringen kan gjelde ett eller flere spesifikke telefon- eller IMEI-numre, eller masteinformasjon, i ett spesifisert tidsrom. PT vurderer denne, og faxer sin avgjørelse tilbake til politiet etter en saksbehandlingstid på 1-2 dager. Politiet sender så kopi av PTs vedtak til den aktuelle teleoperatør, og ber om at de legger frem de aktuelle trafikkdata. Teleoperatøren sender en telefax til politiet med trafikkdata fra all inn- og utgående trafikk for det telefon- eller IMEI-nummer i tidsrommet fritaket gjelder, og har dermed forklart seg ihht. straffeprosessloven § 230.

Et spørsmål i forbindelse med utlevering av trafikkdata på grunnlag av fritak fra taushetsplikten, er om fritaket gjelder både inngående og utgående trafikk. I praksis utleverer teleoperatørene begge typer, men det er ikke klart at dette uten videre er omfattet av fritaket. Som hovedregel gis fritak for trafikkdata for ett eller flere spesifikke SIM- eller IMEI-nummer. I slike tilfeller må utgangspunktet være at det kun er de data som etter konsesjonen er å anse som trafikkdata for disse numre som kan utleveres. Dette betyr at utgående trafikk, samt inngående trafikk som utgjør fakturainformasjon, er omfattet av fritaket, jf. pkt. 2.1.1.1. Hvis det derimot spesifikt er begjært fritak for både inn- og utgående trafikk, står PT fritt til å gi slike fritak. I så fall vil teleoperatøren i tillegg kunne utlevere inngående trafikkdata i den utstrekning de også er utgående trafikkdata fra den samme teleoperatør. Begrunnelsen for denne sondringen er at inngående trafikkdata er taushetsbelagte personopplysninger om andre personer, som eventuelt krever særskilt grunnlag for utlevering. Spørsmålet om data

som er lagret og utlevert i strid med konsesjonen eventuelt kan brukes som bevis er et straffeprosessuelt spørsmål som faller utenfor denne oppgaven.

Grunnlaget for PTs vurdering er straffeprosessloven § 118 første ledd, som slår fast at samtykke bare kan nektes dersom fremleggelsen av de aktuelle trafikkdata vil kunne utsette staten eller allmenne interesser for skade, eller virke urimelig overfor den som har krav på hemmelighold. PT har uttalt[19] at de i slike avgjørelser vurderer styrken på mistanken, hvilken bevisverdi opplysningene har for saken, hvorvidt det finnes mindre inngripende tiltak som politiet bør prøve først og hvor sterk eller sannsynlig forbindelsen mellom et gitt abonnement og en konkret siktet eller mistenkt person er.

Av disse forhold fremstår den eneste vurderingen PT kan ta på noenlunde sikkert grunnlag å være om det finnes mindre inngripende tiltak politiet bør prøve først, basert på informasjon om hva som er gjort tidligere i saken. De øvrige vurderinger; styrken på mistanken, hvilken bevisverdi opplysningene har for saken og hvor sterk eller sannsynlig forbindelsen er mellom et gitt abonnement og en konkret mistenkt, kan etter omstendighetene kreve langt mer inngående informasjon om saken enn det PT sitter inne med. Bortsett fra tilfeller hvor det foreligger tilståelser, hvor det er åpenbart at trafikkdata vil være avgjørende bevis eller med mindre det er snakk om å kontrollere vedkommende som er registrert som eier av et abonnement, er dette vurderinger det kan være usikkert om PT som organ har faglig kompetanse til å ta stilling til. Den begrensede mengde informasjon PT får fra politiet til å basere sin avgjørelse på må dessuten sees i lys av at mistenkte ikke har fått anledning til kontradiksjon.

De beste grunner tilsier derfor at PT i tvilstilfeller burde legge mest vekt på om det finnes mindre inngripende tiltak politiet først burde prøve, og deretter om det foreligger tilstrekkelig mistanke. Hvis disse vilkårene ikke er oppfylt, bør fritak uansett ikke tillates. Deretter kan PT eventuelt vurdere om bevisverdien og sammenhengen mellom mistenkte og det aktuelle telefonnummer er sterk nok til å tillate fritak fra taushetsplikten. Dette vil innebære at vilkårene i straffeprosessloven § 170a i størst mulig grad er oppfylt.

---

[19] Juristkontakt nr. 2, 2003 s. 22.

PT foretar ved slike avgjørelser en vurdering av slik karakter som normalt ligger innenfor domstolenes arbeidsområde, og retten er i straffeprosessloven § 118 annet ledd gitt kompetanse til ved kjennelse å bestemme at vitneforklaring skal gis selv om PT nekter å gi samtykke, eller at vitneforklaring ikke skal mottas selv om PT har samtykket, jf. pkt. 5.2.2. Pkt. 5.2.3 inneholder en drøftelse av problemer knyttet til utlevering av trafikkdata etter både straffeprosessloven § 118 første og annet ledd.

5.2.2 Vitneforklaring som følge av rettens kjennelse

Den avgjørelse PT tar i forhold til taushetsplikten etter straffeprosessloven § 118 første ledd, kan med hjemmel i annet ledd overprøves av domstolene. I praksis er dette mest aktuelt dersom PT nekter å gi fritak. Følgen av at retten ved kjennelse eventuelt beslutter at teleoperatør likevel skal fritas fra sin taushetsplikt er, til forskjell fra ved PTs beslutning, at teleoperatøren samtidig har fått plikt og ikke bare anledning til å forklare seg for politiet, jf. straffeprosessloven § 108. Før retten tar slik avgjørelse, skal den gi departementet anledning til å redegjøre for grunnene for sitt standpunkt. Videre følger det av straffeprosessloven § 118 annet ledd, siste setning, at departementets redegjørelse ikke skal meddeles partene, og av tredje ledd at vitnesbyrdet bare skal meddeles retten og partene i møte for stengte dører og under pålegg om taushetsplikt, jf. § 117 annet ledd. Domstolenes overprøvingsrett anvendes sjelden, både fordi PT godkjenner de fleste begjæringer om fritak fra taushetsplikten og fordi de få begjæringer som ikke godkjennes kun i liten utstrekning bringes inn for retten. Omfanget av trafikkdata som kan utleveres i disse tilfeller må antas å være det samme som ved utlevering etter fritak fra PT, jf. pkt. 5.2.1 og 2.1.1.1.

5.2.3 Felles om forklaring eller utlevering etter strpl. § 118

Det er et par forhold det kan stilles spørsmålstegn ved i forbindelse med PTs avgjørelse, og alternativt rettens kjennelse, om fritak fra taushetsplikt som grunnlag for utlevering av trafikkdata etter straffeprosessloven § 118. Som jeg tidligere har påpekt har slike avgjørelser akkurat den samme virkning for abonnenten som om utleveringen hadde vært et tvangsmiddel, men fordi særskilt vitneplikt etter straffeprosessloven § 118 ikke er faller inn under straffeprosesslovens fjerde del, medfører det til dels betydelige rettssikkerhetsmessige forskjeller.

For det første er verken retten eller PT i slike tilfeller pålagt å vurdere forholdsmessigheten etter straffeprosessloven § 170a, eller det ulovfestede opportunitetsprinsippet, jf. pkt. 5.3.1. I praksis vil nok vurderingene foretatt av retten og PT være relativt like, uavhengig av om det formelt er snakk om bruk av tvangsmidler eller ikke, men det vil ikke være en saksbehandlingsfeil om vurderingen er utelatt.

For det andre blir abonnenten i prinsippet aldri opplyst om at personopplysninger om ham er utlevert fra teleoperatøren i tilfeller hvor utleveringen ikke er et tvangsmiddel. Regelen om plikt til forhåndsvarsling og underretning av parter, jf. forvaltningsloven §§ 16 og 27, gjelder ikke for slike avgjørelser fattet av PT, jf. § 4 første ledd bokstav b. Heller ikke teleoperatørene som står for utleveringen, eller politiet som er mottaker, syntes å ha noen lovbestemt plikt til å informere abonnenten. Teleoperatøren, som står for innsamling av personopplysninger fra den registrerte, er i forbindelse med innsamlingen forpliktet til å informere abonnenten om at utleveringen kan skje, jf. personopplysningsloven § 19 bokstav c. Denne regelen innebærer dog ingen plikt til å underrette ved faktisk utlevering. Poenget ved forhåndsvarsling etter § 19 c er at abonnenten skal kunne avgjøre om han er villig til å utsette seg for risiko for å få opplysninger utlevert eller ikke[20]. Hjemmel til å unnlate slik opplysning finnes i personopplysningsloven § 23 b, som bestemmer at opplysningsplikten ikke omfatter opplysninger det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger. På denne bakgrunn har teleoperatørene verken plikt til å informere abonnenten om at informasjonen som blir lagret kan bli utlevert, eller når slik utlevering konkret skjer. Politiet, som etter hovedregelen i personopplysningsloven § 20 første ledd får plikt til å informere abonnenten, er unntatt fra dette på grunn av det samme unntaket i § 23 b. På den annen side kan det heller ikke sies å foreligge noe forbud mot å opplyse abonnenten om utlevering, men informasjon til mistenkte er etter dette i prinsippet overlatt til politiets eller påtalemyndighetens skjønn. Dette er i sterk kontrast til hvordan det ville ha vært dersom politiet hadde valgt, eller blitt tvunget til, å benytte tvangsmidler. I slike tilfeller stiller straffeprosessloven strenge vilkår for slik utsettelse, jf. pkt. 5.3.2 og 5.3.3, og det

[20] Jf. Johansen 2001 s. 158 flg.

er et krav at retten avsier kjennelse i saken. Fullstendig unnlatelse av slik meddelelse er kun aktuelt i saker om straffeloven kapittel 8 og 9, jf. straffeprosessloven § 208a annet ledd, § 210c annet ledd og § 216j.

For det tredje har mistenkte alltid krav på å få oppnevnt en forsvarer etter straffeprosessloven § 100a første ledd, i saker hvor det er snakk om utsatt underretning om utlevering av trafikkdata med grunnlag i et straffeprosessuelt tvangsmiddel. Oppnevningen av forsvarer skal bl.a. avhjelpe den manglende mulighet til kontradiksjon som følger av utsatt underretning, men i tilfeller hvor det for eksempel blir gitt fritak fra taushetsplikten etter straffeprosessloven § 118 får den mistenkte ikke oppnevnt forsvarer.

Det er vanskelig å se noen god begrunnelse for at siktedes eller mistenktes rettigheter i slike tilfeller skal være forskjellige, avhengig av om teleoperatørene frivillig forklarer seg for politiet eller ikke. I lys av at dagens praksis er at teleoperatørene i prinsippet heller aldri motsetter seg å avgi forklaring, er det grunn til å vurdere om rettssikkerheten er tilstrekkelig ivaretatt med den gjeldende ordning. I en del saker blir dog denne betenkeligheten svekket av det faktum at politiet først ber om utlevering av trafikkdata etter at andre etterforskningsskritt er foretatt. I disse tilfellene har retten som regel allerede foretatt en vurdering av mistanken mot siktede, for eksempel ved å beslutte ransaking etter straffeprosessloven § 197, jf. § 192, eller varetektsfengsling etter straffeprosessloven § 184, jf. §§ 171 flg. Når PT kan legge slike vurderinger foretatt av retten til grunn for sin avgjørelse om å frita teleoperatør fra taushetsplikten eller ikke endres bildet noe, men dette et klart mindretall av sakene.

5.2.4 Samtykke fra abonnent

Det enkleste grunnlaget for utlevering av trafikkdata er at abonnenten samtykker til at teleoperatøren utleverer dataene. Samtykke er i seg selv tilstrekkelig for at politiet kan kreve trafikkdata utlevert fra teleoperatørene, jf. ekomloven § 2-9 første ledd andre setning, som slår fast at taushetsplikten ikke gjelder overfor ”andre enn de som opplysningene gjelder”. Den lovbestemte taushetsplikten gjelder følgelig ikke overfor brukeren av den aktuelle mobiltelefon. Videre er det lagt til grunn i Ot.prp. 58 (2002-2003), side 92, at ”behandling” som krever samtykke som nevnt i § 2-7 annet ledd,

inkluderer enhver bruk av trafikkdata, herunder utlevering. Følgen av at taushetsplikten ikke gjelder når det foreligger samtykke, er at forbudet mot å ta imot forklaring i strid med lovbestemt taushetsplikt i straffeprosessloven § 118 første ledd heller ikke gjelder.

Bruk av samtykke som utleveringsgrunnlag er likevel ikke alltid praktisk. For det første innebærer innhentingen av samtykke at politiets etterforskning mot abonnenten blir avslørt, og for det andre er ikke mistenkte alltid villig til å samarbeide med politiet. I praksis blir samtykke som regel hentet inn i forbindelse med at mistenkte er i avhør hos politiet.

Fordi trafikkdata er personopplysninger, jf. i pkt. 2.1.1, stilles det krav om at samtykket er frivillig, uttrykkelig og informert, og at den opplysningene gjelder avgir erklæring om at han eller hun godtar behandling av opplysninger om seg selv, jf. personopplysningsloven § 2 nr. 7. Telenor og Netcom stiller som vilkår for slik utlevering til politiet at samtykke fra mistenkte skal være skriftlig og underskrevet, og det finnes standardskjemaer for samtykke som i stor utstrekning benyttes. Samtykke medfører derfor at politiet kan få utlevert trafikkdata uten at de vanlige betenkeligheter og lovskranker virker inn på avgjørelsen.

Det er to problemer som reiser seg i forhold til samtykke. For det første er det problematisk å utlevere trafikkdata om inngående trafikk til privatpersoner, fordi dette samtidig innebærer en utlevering av personopplysninger om andre personer som etter avtale om hemmelig telefonnummer kan være taushetsbelagt. Dersom den som ringte opp hadde avtalebasert hemmelig nummer[21] vil dette ikke være filtrert vekk ved utlevering av trafikkdata, og slik utlevering vil medføre brudd på taushetsplikten, jf. ekomloven § 2-9, første ledd, jf. tredje ledd. Til tross for at privatpersoner etter personopplysningsloven § 18 annet ledd, bokstav a, antakelig har krav på informasjon

[21] Avtalebasert hemmelig telefonnummer er ikke det samme som å reservere seg mot nummervisning ved oppringning. Overfor kunder som bare har reservert seg mot nummervisning ved oppringning har teleoperatør i prinsippet ikke noen taushetsplikt om telefonnummer ved utlevering av trafikkdata eller i andre sammenhenger. Fordi inngående trafikkdata uansett ikke utleveres til privatpersoner får ikke forskjellen noen praktisk konsekvens.

om både inn og utgående trafikkdata kun i kraft av at disse er lagret[22], tolker både Netcom og Telenor ekomloven slik at privatpersoner bare får informasjon om utgående trafikkdata når de ber om innsyn i egne samtaleopplysninger.

Spørsmålet er etter dette hvilke trafikkdata politiet kan få utlevert på grunnlag av samtykke, altså om politiet er begrenset til å motta de data abonnenten faktisk får utlevert, eller de kan få data for både inn- og utgående trafikk. Både Telenor og Netcom har som praksis at når politiet ber om utlevering av trafikkdata som følge av samtykke fra mistenkte, utleverer de trafikkdata om både inn- og utgående kommunikasjon. Begrunnelsen er at grunnlaget for å holde informasjon om inngående trafikk hemmelig ikke gjør seg gjeldende overfor politiet, jf. ekomloven § 2-9 tredje ledd.

Praksis med å ikke begrense mengden av data politiet får utlevert på grunn av unntaket fra taushetsplikten i § 2-9 tredje ledd fremstår som korrekt. Likevel kan samtykke fra abonnenten ikke medføre at politiet kan få utlevert andre trafikkdata enn de som er lovlig lagret på abonnenten, jf. pkt. 2.1.1.1. De hensyn som taler for at den personopplysningene gjelder etter personopplysningsloven § 18 annet ledd, bokstav a, kan kreve å få se alt som er lagret, uavhengig av om dette er lagret i medhold av lov eller ikke, gjør seg ikke gjeldende overfor politiet. Derimot er det sterke rettssikkerhets- og personvernmessige argumenter som taler mot at en persons samtykke kan medføre at politiet får tilgang taushetsbelagte opplysninger om andre personer.

For det andre er det ofte slik at et mobiltelefonabonnement er registrert i ett navn, for eksempel foreldre eller en arbeidsgiver, samtidig som det er en annen som er brukeren av telefonen, henholdsvis et barn eller en ansatt. I slike tilfeller kan det være et spørsmål om hvem som skal kunne gi samtykke til at politiet kan innhente trafikkdata fra teleoperatørene. Etter ordlyden i ekomloven § 2-9 innebærer taushetsplikten at teleoperatørene ”plikter å gjennomføre tiltak for å hindre at andre enn de som opplysningene gjelder for får anledning til selv å skaffe seg kjennskap til slike opplysninger”. Spørsmålet blir følgelig hva som ligger i begrepet ”de som opplysningene gjelder for”. En normal språklig forståelse av ordlyden tilsier at slik

[22] Schartum 2004 s. 153-154.

informasjon, som etter personopplysningsloven er å anse som personopplysninger, ikke gjelder for noen andre enn brukeren. Videre er grunnlaget for taushetsplikten brukerens rett til privatliv og hemmelig kommunikasjon, noe ingen andre privatpersoner kan sies å ha noen rett eller beskyttelsesverdig interesse i å kunne forføye over. Dette taler for at juridisk eier av et abonnement ikke har kompetanse til å gi slikt samtykke. Ot.prp. nr. 58 (2002-2003), side 92, legger til grunn at det bare er brukeren som kan samtykke til "annen behandling" av trafikkdata ihht. § 2-7, annet ledd. Det er ingen hensyn som taler for at det skal være forskjell på hvem som kan samtykke til utlevering etter § 2-9 og annen annen behandling etter § 2-7.

Teleoperatørenes praksis er i tråd med denne tolkning, og de utleverer ikke trafikkdata på grunnlag av samtykke fra andre enn den som er registrert som bruker av et abonnement. I realiteten hender det likevel at det er andre enn rette vedkommende som samtykker, særlig i tilfeller hvor det ikke fremgår at eier og bruker av et abonnement er to forskjellige personer. Konsekvensen av dette må være at vedkommende som feilaktig har samtykket derved har medvirket til brudd på ekomloven § 2-9, og etter omstendighetene kan straffes etter § 4-12. I praksis vil det være svært vanskelig å unngå risiko for at andre enn brukeren samtykker så lenge denne informasjonen ikke er registrert hos teleoperatøren.

5.2.5 Nødrett

Utlevering av trafikkdata er ofte en sak som haster. Behovet for å få dataene raskt kommer da i konflikt med de formelle krav som stilles til bruk av tvangsmidler, og den saksbehandlingstid som i andre tilfeller må påregnes fra PT og teleoperatørene. Normal saksbehandlingstid ved begjæring om utlevering av trafikkdata er i dag 1-2 dager for å få godkjennelse fra PT, og deretter 2-3 dager hos teleoperatør. En begjæring om utlevering av trafikkdata begrunnet i nødrett kan i dag behandles i løpet av minutter. I saker hvor det er snakk om å påberope seg nødrett overfor teleoperatørene er det i praksis spørsmål om sporing ved hjelp av trafikkdata i sanntid, jf. pkt. 4.5, altså nødrett som et alternativ til bruk av straffeprosessloven § 216b, jf. pkt. 5.3.3.

Nødrett er en straffrihetsgrunn, altså en hjemmel som gjør en ellers straffbar handling straffri. I slike saker er det teleoperatørenes ulovlige brudd på den lovbestemte

taushetsplikt etter ekomloven § 2-9 som er den straffbare handling, jf. ekomloven § 12-4, annet ledd, jf. tredje ledd. Nødrettsregelen i straffeloven § 47 åpner for at teleoperatører, uten tillatelse fra PT eller rettens kjennelse, kan utlevere trafikkdata for å redde personer eller formuesgjenstander fra en fare de ikke på annen måte kunne komme seg unna, forutsatt at omstendighetene berettiget dem til å anse faren som særdeles betydelig i forhold til den skade som utleveringen av trafikkdata kan forvolde. Nødrettsregelen inneholder etter dette tre vilkår: Det må foreligge en fare, faren må ikke kunne avverges på annen måte og det må foreligge en betydelig interesseovervekt. Begrepet fare er meget vidt, og kan i prinsippet være enhver trussel mot person eller gods. Vilkåret om fare avgrenser dog bruk av nødrett mot å oppnå en fordel[23], nødrettshandlingen må gjøres for å faktisk redde noen fra en truende eller eksisterende fare, jf. ordlyden i straffeloven § 47 første ledd. Videre følger det av vilkåret om interesseovervekt at faren må anses som særdeles betydelig i forhold til den skade vedkommende som blir utsatt for sporingen lider ved denne. Det er derfor viktig å huske at retten til personvern isolert sett står meget sterkt, noe den lovbestemte taushetsplikt i ekomloven § 2-9 er et uttrykk for. I praksis er det vilkårene om fare og interesseovervekt som etter forholdene vil være de faktiske skranker for nødrettslig bruk av trafikkdata til sporing i sanntid. Vilkåret om at faren på annen måte må være uavvendelig kan etter rettspraksis ikke leses bokstavelig. Det vil etter forholdene være tilstrekkelig at den som befinner seg i en nødrettssituasjon velger den rimeligste utvei[24]. Sporing ved hjelp av trafikkdata vil i praksis ofte være den rimeligste måte når politiet har akutt behov for å spore noen opp.

I situasjoner hvor det for eksempel er snakk om å spore opp ett kidnappingsoffer syntes vilkårene for bruk av nødrett klart å være oppfylt, det samme gjelder situasjoner hvor man med meget høy grad av sikkerhet mistenker at en person skal utføre et drap eller en annen alvorlig kriminell handling[25]. Felles for disse situasjonene er at nødretten blir brukt for å avverge eller stoppe en kriminell handling som utgjør en klar fare. Det er

[23] Rt. 1984 s. 1378

[24] Eskeland 2000, s. 229-230

[25] Konsekvensen av slik bruk av sporing etter påberopelse av nødrett medfører i praksis preventiv bruk av et straffeprosessuelt tvangsmiddel, jf. strpl. § 224. Dette kan likevel ikke føre til at bruken er ulovlig.

prinsippielt viktig å skille slike saker fra tilfeller hvor politiet f.eks. ønsker å spore opp en kriminell på rømmen. I slike tilfeller må det legges til grunn at det skal mye til for at en skal kunne si at det foreligger en faresituasjon, og forholdsmessigheten mellom den skade vedkommende lider må veies mot en tenkt situasjon det knyttes sterk usikkerhet til. Det syntes å være tvilsomt om sporing av mistenkte på grunnlag av nødrett kan brukes på denne måten. Det er som regel snakk om personer som kun forsøker å komme seg unna politiet, og det må kunne legges til grunn at det sjelden er tilstrekkelig grunnlag til å mistenke at disse umiddelbart vil begå nye handlinger som medfører fare. En mellomting er tilfeller hvor politiet påberoper seg nødrett for å spore opp stjålne gjenstander, f.eks. en meget kostbar bil eller et smykke. Det kan i slike situasjoner etter omstendighetene sies å være en fare for at godset kan ødelegges eller tapes, men interesseavveiningen tilsier at det må stilles meget høye krav til verdien på gjenstanden. I slike tilfeller vil det dessuten lettere kunne finnes alternative måter å avverge faren på.

Loven stiller ingen krav til verken form eller innhold ved påberopelse av nødrett, naturligvis det er lite praktisk å i ”normale” situasjoner å påberope seg dette før man foretar handlingen. Både Netcom og Telenor krever likevel slike henvendelser skriftlig eller skriftlig bekreftet, de forlanger at politiet uttrykkelig påberoper seg nødrett og at begjæringen er signert av jourhavende politijurist eller vaktsjef.

Teleoperatørene får mange henvendelser som er på, og av og til langt utenfor, grensene for når nødrett lovlig kan påberopes. Dette medfører flere problemer. For det første er det klart at det som regel er mennesker uten noen form for juridisk kompetanse som tar imot nødrettsbegjæringer hos teleoperatørene, og de ikke er i stand til å vurdere om begjæringen er lovlig eller ikke. For det andre er det liten tvil om at teleoperatørene, uansett faglig kompetanse, i kraft av å være en tjenesteleverandør verken kan eller bør kontrollere og eventuelt overprøve politiets vurderinger i slike saker. For det tredje finnes det ingen regler for etterfølgende kontroll av nødrettssakene, hvilket medfører at det ikke blir opprettet noen grenser for lovlig praksis ved slik bruk av trafikkdata.

Høsten 2002 ble det opprettet et samarbeidsforum mellom politiet og teleoperatørene, bestående av en ledelsesgruppe og en teknisk gruppe[26]. Begge gruppene ledes av Politidirektoratet og består for øvrig av deltakere fra Telenor, Netcom, Oslo politidistrikt, Politiets sikkerhetstjeneste og Politiets datakrimsenter (Økokrim). På et møte i dette samarbeidsforumet ble det i forbindelse med nødrettsproblematikken uttalt at det er politiet og påtalemyndigheten som er ansvarlig for at de anmodninger og pålegg de sender teleoperatørene er korrekte, og at de har hjemmel i lovverket. Det ble videre sagt at det ikke er teleoperatørenes ansvar eller oppgave å overprøve dette, noe som i de aller fleste tilfeller må antas å være den beste løsningen. Begrunnelsen var at det er politiet og påtalemyndigheten som har kjennskap til saken, og sitter med unik kunnskap om både helheten og alle detaljene. En saksbehandler hos teleoperatørene vil ikke ha tilsvarende kunnskap om saken, og vil derfor vanskelig kunne vurdere politiets beslutning. Ved nødrett ligger det dessuten i sakens natur at det sjelden vil være tid til slik overprøving.

Den vanlige hjemmel for sporing av personer i sanntid er som nevnt straffeprosessloven § 216b, som enten krever rettens kjennelse etter første ledd, eller i hastesaker ordre fra politimesteren. Dersom rettens kjennelse ikke er hentet inn, skal saken forelegges retten for godkjennelse innen 24 timer, jf. straffeprosessloven § 216d. Fordi det i de fleste tilfeller uansett ville være umulig blir nødrettssakene naturligvis ikke lagt frem for retten på forhånd, men de blir heller ikke behandlet som hastesaker etter § 216d. Sakene blir derfor verken forhåndsgodkjent av politimesteren eller retten, og de blir heller ikke forelagt retten for etterfølgende godkjennelse. Dette er i sterk kontrast med de øvrige hjemler og situasjoner for utlevering av trafikkdata.

Betenkelighetene rundt bruk av nødrett som hjemmel for utlevering av trafikkdata forsterkes av omfanget. Nødrettssakene utgjør i dag ca. 20% av de henvendelser teleoperatørene får fra politiet. Antallet nødrettssaker er sterkt stigende, Telenor har for eksempel hatt en økning på flere hundre prosent de siste årene. Fordi det er liten grunn til å tro at antallet saker hvor vilkårene for nødrett foreligger har økt så betraktelig, er

[26] Informasjon om samarbeidsforumet og uttalelser gitt i møter i dette er gitt av Bente Sturruste i Politidirektoratet (POD) den 12.03.04.

det relevant å spørre om alle henvendelser virkelig oppfyller disse vilkårene. En mulig forklaring på økningen er at dette skyldes at politiet tidligere ikke har benyttet seg av mulighetene som ligger i den nye teknologien fullt ut, enten fordi de ikke er klar over at muligheten finnes eller fordi de ikke har visst hvordan de skal gå frem. Antakelig må den største del av økningen tilskrives slike forhold. Den andre muligheten er at politiet i et økende antall saker feilaktig påberoper seg nødrett, enten for å få fortgang i saksbehandlingen eller fordi de ikke er klar over hvilke vilkår som må ligge til grunn før nødrett lovlig kan erklæres. Uavhengig av bakgrunnen for økningen syntes de beste grunner å tale for at utlevering av trafikkdata som følge av at politiet eller påtalemyndigheten har påberopt seg nødrett, burde behandles som tilsvarende hastesaker, jf. § 216d. Dette vil ikke forsinke politiets arbeid når det etter deres oppfatning foreligger en nødrettssituasjon, men sørge for at vurderingene blir kontrollert i ettertid og dermed bidra til å sikre at politiets arbeid er innenfor lovens rammer. Dagens system innebærer at rettslig prøving av politiets begjæringer kun kan skje dersom den vedtaket retter seg mot går til straffesak for brudd på taushetsplikten, jf. ekomloven § 12-4 annet ledd, jf. tredje ledd.

5.3 Utlevering av trafikkdata som straffeprosessuelt tvangsmiddel

I de aller fleste saker vil utgangspunktet for utlevering av trafikkdata være et av de hjemmelsgrunnlag jeg har redegjort for ovenfor. I dag er det kun unntaksvis at trafikkdata blir utlevert som følge av et straffeprosessuelt tvangsmiddel. De tre straffeprosessuelle hjemmelsgrunnlag innebærer dessuten i praksis kun to former for utlevering. Det er enten snakk om tilfeller hvor teleoperatørene nekter å utlevere trafikkdata til tross for at de er fritatt for taushetsplikten, eller tilfeller hvor påtalemyndigheten uten foregående fritak ber om rettens kjennelse for utlevering etter reglene om kommunikasjonskontroll i straffeprosessloven kap. 16a.

Fordi den klare hovedregel er at utlevering av trafikkdata skjer på andre grunnlag enn som følge av et straffeprosessuelt tvangsmiddel, og fordi en grundig redegjørelse for disse reglene ville medføre at denne oppgaven går utenfor de gitte rammer, har jeg valgt å gjøre dette så kort som jeg har funnet forsvarlig. Reglene om beslag og utleveringspålegg er dessuten grundig behandlet i juridisk teori og praksis, og den type generell straffeprosessuell teori faller utenfor temaet for denne oppgaven. I stedet har

jeg valgt å legge vekt på å peke på områder hvor anvendelsen av de straffeprosessuelle reglene i forbindelse med bruk av trafikkdata gir seg spesielle utslag. Reglene om utlevering av trafikkdata som del av kommunikasjonskontroll etter straffeprosessloven kap. 16a krever en noe mer utførlig gjennomgang, bl.a fordi dette er den eneste ordinære hjemmel for kontroll med fremtidige trafikkdata og kontroll i sanntid. Likevel er også denne redegjørelsen holdt på et minimum fordi reglene benyttes svært sjelden i praksis.

5.3.1 Forholdsmessighetsprinsippet

Forholdsmessighetsprinsippet i straffeprosessloven § 170a gjelder alltid ved bruk av lovens fjerde del, uansett hvilket tvangsmiddel det er snakk om. Forholdsmessighetsprinsippet fungerer som en sikkerhetsventil, selv om det for øvrig er hjemmel for å iverksette kommunikasjonskontroll er det ikke dermed sagt at dette kan gjøres. Avhengig av om det er påtalemyndigheten eller retten som bestemmer bruken, må disse foreta en konkret avveining mellom behovet for inngrepet og den skade eller ulempe det vil medføre for den eller de som blir utsatt for det. Regelen stiller opp to kumulative vilkår. For det første må det være tilstrekkelig grunn til bruken av tvangsmidlet, og for det andre må det ikke innebære et uforholdsmessig inngrep.

Utlevering av trafikkdata er ansett som mindre inngripende enn sporing i sanntid, og vil følgelig lettere bli ansett som et forholdsmessig tiltak. Videre er det forskjell mellom de ulike hjemmelsgrunnlag. Saker om kommunikasjonskontroll etter § 216b første ledd bokstav a står i en særstilling på grunn av den høye strafferammen på fengsel i minst fem år. Det er her snakk om meget alvorlig kriminalitet, og tvangsmidler blir følgelig vurdert som mindre inngripende. Derimot vil forholdsmessighetskravet vurderes strengere for saker som faller inn under reglene om beslag, utlevering eller kommunikasjonskontroll etter straffeprosessloven § 216b første ledd bokstav b. Fordi det i disse sakene i utgangspunktet ikke stilles noe krav til strafferamme vil enhver bruk av tvangsmidler måtte vurderes konkret i forhold til den reaksjon som kan forventes. Ved siden av strafferammen er momenter i forholdsmessighetsvurderingen hvor alvorlig saken er, mistankens styrke og hvor viktig kommunikasjonskontrollen er for etterforskningen. Spørsmålet om hvordan utlevering av trafikkdata vil kunne påvirke eller skade mistenkte og dennes rettigheter tillegges stor vekt.

Sporing i sanntid kan kun skje etter reglene om kommunikasjonskontroll med hjemmel i straffeprosessloven § 216b annet ledd, bokstav c. Dette er som nevnt ansett som et mer inngripende tiltak enn ordinær utlevering av trafikkdata, og det er følgelig mer som taler mot å anvende inngrepet. På grunn av den forskjell i vurderingen mellom saker hjemlet i første ledd bokstav a og bokstav b som nevnt i forrige avsnitt syntes sporing i sanntid kun å være aktuelt i forbindelse med bokstav a, eller de mest alvorlige tilfeller som faller inn under bokstav b.

For utlevering etter reglene om kommunikasjonskontroll finnes det i § 216f krav om at tillatelse til dette kun skal gis for et bestemt tidsrom som ikke må være lenger enn strengt nødvendig. For beslag og utlevering finnes det ingen tidsmessig begrensning i loven, og avgjørelsen av de tidsmessige rammer er derfor i slike saker en viktig del av forholdsmessighetsvurderingen.

5.3.2 Utlevering etter reglene om beslag og utleveringspålegg

Fordi fritaket fra taushetsplikten kun gir teleoperatørene anledning til å forklare seg overfor politiet, kan de i prinsippet nekte å gjøre dette, jf. pkt. 5.2.1. Dersom teleoperatøren nekter må politi eller påtalemyndighet da benytte tvangsmidler for å få gjennomført kontroll. Alternativene er reglene i straffeprosessloven §§ 203 eller 210, som bestemmer at ”ting” som kan ha betydning som bevis kan beslaglegges eller pålegges utlevert. Høyesteretts kjæremålsutvalg slo i Rt. 1992 s. 904 fast at trafikkdata lagret hos teleoperatør er å anse som ”ting” ihht. § 203, og at ”ting” tolkes likt for hele straffeprosessloven kapittel 16. Forutsetningen for beslag eller utleveringspålegg er etter dette at teleoperatørene har vitneplikt for retten, jf. straffeprosessloven § 204 første ledd, annen setning, og § 210 første ledd, hvilket er oppfylt som følge av at PT allerede har gjort fritak fra taushetsplikten.

Spørsmålet etter dette er hvilke data som omfattes av beslag eller utleveringspålegg. Fordi det er en forutsetning for å anvende disse tvangsmidlene at PT allerede har gjort fritak fra taushetsplikten, er det på den ene side nærliggende å ta utgangspunkt i de data som omfattes av fritaket, jf. pkt. 5.2.1. På den andre side er vurderingen ved bruk av tvangsmidler ikke knyttet opp opp mot et bestemt nummer eller en bestemt person, men

mot hva som kan ha betydning som bevis i saken. Fordi det i de fleste saker må anses som klart at data fra både inn- og utgående trafikk vil kunne ha stor bevisverdi, taler dette for at også disse data er omfattet. Praksis fra teleoperatørene er i slike tilfeller, som ellers, å utlevere all inn- og utgående trafikkdata.

Som ved begjæring om fritak fra taushetsplikten, jf. pkt. 5.2.1, vil det avgjørende ved begjæring om utleveringspålegg være hva begjæringen går ut på. I lys av at retten etter straffeprosessloven § 118 annet ledd har hjemmel til å overprøve PTs beslutning om fritak, og at reglene om beslag og utlevering gjelder alt som "antas å ha betydning som bevis", må retten på grunnlag av politiets begjæring også etter § 210 kunne bestemme at inngående trafikkdata skal utleveres. Dette gjelder også trafikkdata som teleoperatørene har lagret i strid med konsesjonen[27]. Det samme må gjelde påtalemyndigheten ved beslutning om beslag, jf. § 205 første ledd, som eventuelt kan legge saken frem for retten etter § 205 annet ledd.

Når det blir besluttet beslag eller utleveringspålegg er hovedregelen at mistenkte skal opplyses om dette, jf. § 200 første ledd, jf. § 205 første ledd, siste punktum, og forutsetningsvis § 210a. I de fleste tilfeller er underretning dog unødvendig, fordi slike tvangsmidler som oftest medfører at mistenkte enten må samarbeide, eller på annen måte blir klar over tiltakene. Ved utlevering av trafikkdata vil mistenkte som hovedregel derimot ikke få slik kjennskap, og opplysningsplikten er derfor viktig for å ivareta mistenktes rettssikkerhet. Hvis det er strengt nødvendig for etterforskningen i saken at underretning ikke gis, og abonnenten med skjellig grunn kan mistenkes for en handling eller forsøk på en handling som etter loven kan medføre høyere straff enn fengsel i 6 måneder, kan politi eller påtalemyndighet likevel etter §§ 208a og 210a be om rettens kjennelse for å utsette underretningen til mistenkte. Ved behandlingen av spørsmål om utsatt underretning har mistenkte krav på oppnevning av hemmelig forsvarer, jf. § 100a.

Utlevering av trafikkdata som følge av straffeprosesslovens regler om beslag eller utleveringspålegg blir lite brukt i praksis. Av hensyn til kundens rett til privatliv og

[27] Spørsmålet om beslaglagte eller utleverte trafikkdata som er lagret i strid med konsesjonen kan benyttes som bevis, er et straffeprosessuelt spørsmål som faller utenfor rammene av denne oppgave.

hemmelig kommunikasjon krevde Netcom frem til høsten 2002 alltid rettens kjennelse etter straffeprosessloven § 210 før de utleverte trafikkdata, men fordi retten i praksis alltid aksepterte begjæringer godkjent av PT ble dette kravet bare en formell skranke som forsinket prosessen. I dag er det svært sjelden at Telenor eller Netcom ikke frivillig utleverer trafikkdata etter å ha blitt fritatt fra taushetsplikten.

5.3.3 Utlevering etter reglene om kommunikasjonskontroll

Straffeprosessloven har i kapittel 16a spesielle regler for kommunikasjonskontroll som tvangsmiddel. Hjemmelen for kontroll av trafikkdata er straffeprosessloven § 216b annet ledd, bokstav c. Etter denne regelen kan kontrollen gå ut på "hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg som nevnt i bokstav a, og andre data knyttet til kommunikasjon." Ifølge Ot.prp. nr. 64 1998-1999 om lov om endringer i straffeprosessloven og straffeloven mv (etterforskningsmetoder m.v.), side 159, omfattes trafikkdata av "andre data knyttet til kommunikasjon". Med hjemmel i denne regelen kan retten, uavhengig av om teleoperatørene på forhånd er fritatt fra taushetsplikten, pålegge utlevering av historiske trafikkdata, fremtidige trafikkdata eller sporing ved hjelp av trafikkdata i sanntid.

Grunnvilkåret for tillatelse til bruk av kommunikasjonskontroll etter § 216b er skjellig grunn til mistanke om straffbart forhold som kan medføre fengsel i 5 år eller mer, jf. første ledd bokstav a. Dessuten kan slik kontroll gjennomføres dersom mistanken dreier seg om et av de straffebud som nevnt i bokstav b, herunder bestemmelsene om narkotikakriminalitet, organisert kriminalitet og barnepornografi.

Nærmere vilkår for kommunikasjonskontroll følger av § 216c, som i første ledd krever at kontrollen må antas å være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad blir vanskeliggjort. Det er i teorien[28] antatt at det i disse vilkår ligger et krav om at kommunikasjonskontroll bare kan benyttes når andre metoder ikke strekker til. Mobiltelefoner vil i praksis svært sjelden falle inn under regelen i annet ledd første setning, men dersom telefonen tilhører advokat, prest, lege

[28] Bjerke 2001, s. 748.

eller annen som erfaringsmessig fører samtaler av svært fortrolig art kreves det etter annen setning dessuten særlige grunner for at kontroll kan tillates. Særlige grunner kan for eksempel være hvor alvorlig den straffbare handling er. For øvrig må tilleggsvilkårene i § 216c sees i sammenheng med forholdsmessighetsprinsippet i § 170a, jf. pkt. 5.3.1.

Underretning om kommunikasjonskontroll gis kun på begjæring, og tidligst ett år etter at kontrollen er avsluttet, jf. § 216j. Ved behandling av saker etter § 216b er kontradiksjon sikret ved at mistenkte her rett til hemmelig forsvarer, jf. § 100a.

Reglen i § 216b annet ledd, bokstav a, bestemmer hva kontrollen kan rettes mot. Denne regelen bestemmer at kontroll kun kan foretas mot bestemte telefoner, som den mistenkte besitter eller kan antas å ville bruke. Dette spesifikasjonskravet finnes ikke i de øvrige hjemler for utlevering av trafikkdata, og begrenser anvendelsesområdet til kommunikasjonskontroll i forhold til disse. Dette innebærer at politiet for eksempel ikke kan få utlevert opplysninger om hvilke telefoner som har vært koblet til en spesifikk basestasjon i et gitt tidsrom (basestasjonsøk, jf. pkt. 4.3). I forhold til hvilke trafikkdata som kan utleveres på grunnlag av kjennelse om kommunikasjonskontroll, medfører spesifikasjonskravet at det ikke kan utleveres andre data enn de som utgjør faktureringsinformasjon for det telefon- eller IMEI-nummer kjennelsen gjelder. Data fra all inngående fra kommunikasjon når abonnenten befinner seg i Norge faller dermed utenfor § 216b, jf. pkt. 2.1.1.1.

I praksis forekommer utlevering av trafikkdata etter disse reglene nesten bare i forbindelse med, og som et supplement til, kommunikasjonsavlytting etter straffeprosessloven § 216a. Det er vanskelig å si noe sikkert om hvorfor straffeprosessloven § 216b brukes så sjelden, men det kan ha sammenheng med at regelen er relativt ny og ukjent. Dessuten fremstår regelen som vesentlig vanskeligere å benytte enn de øvrige hjemler for utlevering av trafikkdata, uten at den gir særlige ”fordeler”. Vilkårene for bruk av straffeprosessloven § 216b er vesentlig strengere enn de øvrige hjemler, og konsekvensene, som for eksempel at påtalemyndigheten ikke behøver å få rettens kjennelse om utsatt underretning, jf. straffeprosessloven § 216i, har liten betydning fordi slik utsettelse uansett er praksis i de fleste saker hvor det er behov

for det. Utlevering av historiske trafikkdata, som er den klart mest brukte formen for slik kontroll, kan dessuten ordnes med en rekke andre hjemler. Selv om de strenge vilkår til strafferamme etter straffeprosessloven § 216b er oppfylt er det upraktisk å be om rettens kjennelse der hvor man kan nøye seg med tillatelse fra PT. Utlevering av fremtidige trafikkdata, hvor straffeprosessloven § 216b er den eneste hjemmel, er heller ikke så praktisk at politiet velger å bruke denne hjemmelen. I realiteten vil teleoperatøren selv med pålegg for fremtiden bare sende trafikkdata til politiet med jevne mellomrom etter at de har kommet inn, slik at politiet i mange tilfeller like gjerne kan innhente fritak fra PT hver gang de har behov for nye data. Straffeprosessloven § 216b er også den eneste ordinære hjemmelen for sporing av mistenkte i sanntid, men fordi politiet sjelden på forhånd vet at de får behov for sporing slik at de kan innhente rettens tillatelse, blir dette enten ikke gjennomført eller i stedet begjært med hjemmel i nødrettsparagrafen i straffeloven § 47, jf. pkt. 5.2.4.

Det fremstår som uheldig fra et rettssikkerhetsmessig synspunkt at den lovbestemte beskyttelse mistenkte ville ha fått dersom utlevering hadde skjedd på grunnlag av reglene om kommunikasjonskontroll, kun kommer til anvendelse i svært få saker, jf. pkt. 5.2.3.

6 Avsluttende bemerkninger

Generelt syntes det å være relativt dårlig sammenheng mellom regelverk og praksis på området lagring og bruk av trafikkdata. Grunnene til dette kan være mange, men et uoversiktlig retskildebilde, til dels sterke motstridende interesser og tekniske løsninger som ikke er tilpasset lovgivningen syntes å være de mest fremtredende.

I forhold til reglene om lagring av trafikkdata er spørsmålet om lovgiver burde vedta plikt til å lagre i en bestemt periode vesentlig. Dette er et vanskelig spørsmål som krever en grundig vurdering, men det er ikke tvil om at mange av de problemene teleoperatørene har i forhold til Datatilsynets konsesjonsvilkår og lovgivingen i dag skyldes den utstrakte plikten til å slette. Det faktum at teleoperatørenes lagring syntes å være i dårlig overensstemmelse med regelverket er ikke i seg selv noe argument for å endre loven, men kan sees som et uttrykk for at det er behov for en endring. Uavhengig av eventuelle lovendringer syntes det å være behov for at Datatilsynets konsesjonsvilkår endres slik at de inneholder spesifikke regler om lagring av trafikkdata fra kunder med forhåndsbetalte abonnement.

Når det gjelder bruk av trafikkdata er det etter mitt skjønn viktigst å ta tak i rettssikkerhetsspørsmålet i saker hvor utlevering av trafikkdata skjer på grunnlag av at PT fritar teleoperatøren fra taushetsplikten. Dersom teleoperatøren etter fritak frivillig utleverer trafikkdataene er det intet krav om en forholdsmessighetsvurdering, det er intet krav om rettslig prøving av utsatt underretning og vedkommende som blir utsatt for kontrollen har ingen mulighet til kontradiksjon ved oppnevning av hemmelig forsvarer dersom han ikke blir underrettet. Hvis teleoperatørene derimot hadde nektet å utlevere dataene til tross for fritaket, måtte utlevering ha skjedd på grunnlag av reglene om beslag eller utlevering, med den rettssikkerhetsmessig beskyttelse som følger av loven. En slik situasjon hvor teleoperatørene i praksis avgjør abonnentenes rettssikkerhetsmessige beskyttelse er etter min oppfatning lite tilfredsstillende, særlig i lys av at operatørene nesten aldri nekter å utlevere.

Videre fremstår forskjellene i vilkår for bruk og rekkevidde mellom de forskjellige hjemler for utlevering av trafikkdata betenkelig. For det første er rekkevidden av de ikke straffeprosessuelle hjemler videre enn for de straffeprosessuelle, noe som stemmer dårlig overens med de strengere vilkår som stilles til bruk av de sistnevnte. For det andre stilles det ingen særlige vilkår for bruken av de generelle straffeprosessuelle tvangsmidlene beslag og utleveringspålegg i forbindelse med utlevering av trafikkdata, samtidig som vilkårene for de spesielle straffeprosessuelle reglene om kommunikasjonskontroll er så strenge at disse reglene i praksis nesten aldri brukes.

Det siste forhold jeg vil fremheve er problematikken rundt bruk og kontroll av nødrett som grunnlag for utlevering av trafikkdata. Bruken av nødrett er sterkt økende og praksis veldig variert, og uten formell kontroll er det vanskelig for alle aktører å vite hvor grensene går. I lys av de hensyn som ligger bak reglene om etterfølgende kontroll ved bruk av hastekompetanse for utlevering av trafikkdata, syntes det å være et sterkt behov for etterfølgende domstolsprøving også for nødrettssaker.

7 Litteraturliste/kilder

Litteratur:

Andenæs 2000. *Norsk Straffeprosess*, bind II. 3. utgave. Oslo, 2000. Johs. Andenæs.

Bjerke 2001. *Straffeprosessloven kommentarutgave*, bind I. 3. utg. Oslo, 2001. Hans Kristian Bjerke og Erik Keiserud.

Bjerke 2001. *Straffeprosessloven kommentarutgave*, bind II. 3. utg. Oslo, 2001. Hans Kristian Bjerke og Erik Keiserud.

Bjerke, 2002. *Straffeprosessloven tilleggshefte*. 3. utg. Oslo, 2002. Hans Kristian Bjerke og Erik Keiserud (Red.).

Eckhoff 1997. *Forvaltningsrett*. 6. utg. Oslo, 1997. Torstein Eckhoff og Eivind Smith.

Johansen 2001. Personopplysningsloven kommentarutgave. Oslo 2001. Michal Wiik Johansen, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud.

Schartum 2004. Personvern i informasjonssamfunnet. Oslo, 2004. Dag Wiese Schartum og Lee A. Bygrave.

Artikler:

Asle Fuhr, Kjerstin Ringdal og Brynjar Mørkved. *Loven krever fritak fra taushetsplikten* I: Juristkontakt 2:2003 s. 20-23.

Forarbeider:

NOU 2004:6 Om politimetoder i forebyggende øyemed

NOU 2003:27 Lovtiltak mot datakriminalitet

Ot.prp. nr. 64 (1998-99) Om lov om endringer i straffeprosessloven og straffeloven mv

Ot.prp. nr. 58 (2002-2003) Om lov om elektronisk kommunikasjon (ekomloven)

Ot.prp. nr. 62 (2002-2003) Om lov om endringer i straffeloven og straffeprosessloven mv. (lovtiltak mot organisert kriminalitet og menneskehandel, gjengangerstraff mv.)

Internett ressurser:

Karnov Norsk Lovkommentar, http://www.rettsdata.no, 15.04.04

Statistisk årbok 2003, http://www.ssb.no/aarbok/tab/t-101250-519.html, 15.04.04

Bruk av IKT i Husholdningene, http://www.ssb.no/emner/10/03/ikthus/, 15.04.04

Norsk Kriminalstatistikk 2002, http://www.ssb.no/emner/03/05/a_krim_tab/, 15.04.04

Rettsavgjørelser:

Rt. 1984 s. 1378

Rt. 1992 s. 64

Rt. 1992 s. 904

Rt. 1999 s. 1944

Rt. 2000 s. 1236

Vedlegg 1

Datatilsynet

XXXXX
XXXXX
XXXXX
XXXXX

Deres ref	Vår ref (bes oppgitt ved svar)	Dato
	XXXXXXXXXX	XXXXXX

KONSESJON TIL Å BEHANDLE PERSONOPPLYSNINGER – BEHANDLING AV OPPLYSNINGER OM ABONNENTERS BRUK AV TELETJENESTER

Vi viser til Deres søknad av XXXXXX om konsesjon til behandling personopplysninger.

I medhold av Lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 31, 4. ledd, jf. Kgl. Resolusjon av 15. desember 2000 § 7-1, er Deres virksomhet gitt konsesjon til å behandle personopplysninger ved abonnenters bruk av teletjenester. Vilkårene i konsesjonen er gitt i medhold av personopplysningslovens §§ 34 og 35.

Konsesjonen er gitt under forutsetning av at behandlingen foretas i henhold til søknaden og de bestemmelser som følger av personopplysningsloven med forskrifter.

Dersom det skjer endringer i behandlingen i forhold til de opplysninger som er gitt i søknaden, må dette fremmes i ny konsesjonssøknad.

Datatilsynet har i denne konsesjonen fastsatt følgende vilkår for behandlingen:

1. Formålet med behandlingen

Formålet med behandlingen er kundeadministrasjon, opplysningstjeneste, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av telenett, inklusive samtrafikkavregning. Personopplysningene kan bare brukes til disse formål. Dersom opplysningene skal brukes til andre formål, må den behandlingsansvarlige sørge for at dette skjer i henhold til personopplysningsloven.

2. Opplysningstyper

Det kan bare behandles opplysninger som er nødvendige for gjennomføring og fakturering av tjenesten.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50

3. Behandlingsansvarlig

Behandlingsansvarlig er XXXXXXXX.

Det daglige ansvaret for behandlingen ligger hos daglig leder.

Behandlingsansvarlige plikter å sørge for at bestemmelsene i personopplysningsloven med forskrifter, og denne konsesjonen blir fulgt.

4. Behandlingens omfang

Konsesjonen omfatter all behandling av personopplysninger i forbindelse med abonnentenes bruk av telenett. Konsesjonen gjelder for alle typer teletjenester.

Virksomheten skal, der det er mulig, tilby alternative teletjenester hvor det ikke behandles opplysninger om brukeren

5. Innsamling av opplysninger

Opplysningene kan bare innhentes fra abonnenten, og gjennom abonnentens bruk av teletjenester i telenett.

Behandlingsansvarlige skal kontrollere at de innsamlede opplysninger er korrekte, komplette og aktuelle for det formålet de er innsamlet til.

6. Utlevering av opplysninger

Personopplysninger fra må ikke utleveres til utenforstående.

Utlevering kan likevel skje

1. når den opplysningen gjelder har gitt samtykke til det, det vil si en frivillig, uttrykkelig og informert erklæring om at han eller hun godtar utlevering av opplysninger om seg selv.
2. med hjemmel i lov, eller i forskrift gitt med hjemmel i lov,
3. som ledd i betalingsinnkreving (inkasso),
4. som ledd i regnskapsbehandling,

Når utlevering skjer med hjemmel i lov, i forskrift gitt med hjemmel i lov eller etter enkeltvedtak fra Datatilsynet skal den opplysningene gjelder informeres om dette, hvis ikke annet følger av lov. I informasjonen skal det framgå hva som utleveres, til hvilket formål og hvem som er mottaker av opplysningen.

Oppbevaring eller behandling av personopplysninger hos et databehandlingsforetak regnes ikke som utlevering når dette skjer på oppdrag fra den behandlingsansvarlige.

7. Utlevering gjennom katalogutgivelse og opplysningstjeneste

Uten slikt samtykke som nevnt i punkt 6 kan personopplysninger utleveres gjennom utgivelse av trykte eller elektroniske kataloger eller gjennom opplysningstjenester. Det samme gjelder utlevering til andre virksomheter som skal utgi kataloger eller opprette opplysningstjenester. Utleveringen kan bare skje på følgende vilkår:

1. Opplysningene kan bare brukes til utgivelse av trykte eller elektroniske abonnentkataloger eller opprettelse av opplysningstjenester.
2. Virksomheten skal informere abonnenten om oppføringen i katalog og opplysningstjenesten, om at abonnenten kan reservere seg mot å bli oppført og om at han eller hun vil bli oppført dersom vedkommende ikke reserverer seg.
3. Abonnenten skal gis en rimelig frist til å reservere seg mot oppføringen.
4. Bare opplysninger som er nødvendig for å identifisere en bestemt abonnent kan utleveres. Skal ytterligere opplysninger oppføres, gjelder regelen om samtykke i punkt 6 nr 1.

Abonnenten kan kostnadsfritt kreve å bli utelatt fra en trykt eller elektronisk katalog eller opplysningstjeneste, at vedkommendes adresse delvis utelates, at opplysningene ikke brukes til direkte markedsføring og at det ikke framgår av katalogen eller tjenesten om vedkommende er mann eller kvinne når dette ikke framgår av abonnentens navn i seg selv.

8. Sletting av opplysninger

Generelt om sletting

Den behandlingsansvarlige skal slette eller anonymisere opplysninger som ikke har betydning for formålet.

Den behandlingsansvarlige skal av eget tiltak rette, slette eller supplere opplysninger som er uriktige eller ufullstendige, dersom feilen eller mangelen har betydning for den opplysningene gjelder.

Har feilen eller mangelen ført til at uriktige eller ufullstendige opplysninger er levert ut eller brukt, skal behandlingsansvarlige sørge for at dette så vidt mulig ikke kan få betydning for den opplysningene gjelder. Vedkommende skal informeres om feilen snarest mulig.

Slettefrist

Opplysninger som benyttes til faktureringsformål, skal slettes når faktura er gjort opp, eventuelt når en klagefrist er gått ut. Ved kvartsvis fakturering skal opplysningene slettes senest fem - 5 måneder etter at de ble registrert. Velger virksomheten å gå over til månedsvis fakturering, skal opplysningene slettes senest tre – tre måneder etter at de ble registrert. Dersom en faktura ikke er blitt betalt eller det er oppstått rettslig tvist om betalingsplikten, kan opplysningene likevel oppbevares inntil kravet er gjort opp eller rettslig avgjort. Etter at faktura er gjort opp, kan det for faktura perioden lagres navn og adresse på kunden i tillegg til beløpet.

Opplysninger som kun er nødvendig for oppkobling eller gjennomføring av tjenesten, skal slettes straks tjenesten er nedkoblet.

Uavhengig av det ovenstående kan opplysninger som det er nødvendig å oppbevare for å oppnå en tilfredsstillende informasjonssikkerhet, oppbevares så lenge det er påkrevet etter regler i forskriftens kapittel 2 for informasjonssikkerhet ved behandling av personopplysninger § 2-16.

Kravet om sletting etter dette punkt gjelder så langt opplysningene ikke skal oppbevares i henhold til annen lov.

9. Sammenstilling

Med sammenstilling er det i denne konsesjonen ment elektronisk samkjøring av personregistre i den hensikt å opprette et nytt register, eller å tilføre nye typer opplysninger til de personregistre som kobles.

Registeret må ikke sammenstilles med andre personregistre, uten når dette skjer med hjemmel i lov.

Sammenstilling av registre som eies av selskaper innen samme konsern er tillatt, når dette er nødvendig for å gjennomføre formålet med konsesjonen.

10. Faktura

Abonnenten skal gis uspesifisert regning dersom annet ikke er avtalt.

11. Fortsatt behandling

Den behandlingsansvarlige skal hvert tredje år sende Datatilsynet bekreftelse på at behandlingen skjer i overensstemmelse med søknaden og personopplysningslovens regler.

Vedtaket kan påklages. Klagefristen er tre uker. For nærmere informasjon om klageadgangen, se vedlagte skriv.

Med hilsen

Knut-Magnar Aanestad
seniorrådgiver

XXXXXXX
XXXXXXX

Vedlegg:
-Kommentarer til konsesjonen
-Personopplysningsloven
-Forskrifter til personopplysningsloven
-Melding om rett til å klage over forvaltningsvedtak